

EXAMINING DATA SECURITY AT THE UNITED STATES POSTAL SERVICE

HEARING

BEFORE THE
SUBCOMMITTEE ON FEDERAL WORKFORCE,
U.S. POSTAL SERVICE AND THE CENSUS
OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

NOVEMBER 19, 2014

Serial No. 113-157

Printed for the use of the Committee on Oversight and Government Reform



Available via the World Wide Web: <http://www.fdsys.gov>
<http://www.house.gov/reform>

U.S. GOVERNMENT PUBLISHING OFFICE

93-230 PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida	ELIJAH E. CUMMINGS, Maryland, <i>Ranking</i>
MICHAEL R. TURNER, Ohio	<i>Minority Member</i>
JOHN J. DUNCAN, JR., Tennessee	CAROLYN B. MALONEY, New York
PATRICK T. McHENRY, North Carolina	ELEANOR HOLMES NORTON, District of
JIM JORDAN, Ohio	Columbia
JASON CHAFFETZ, Utah	JOHN F. TIERNEY, Massachusetts
TIM WALBERG, Michigan	WM. LACY CLAY, Missouri
JAMES LANKFORD, Oklahoma	STEPHEN F. LYNCH, Massachusetts
JUSTIN AMASH, Michigan	JIM COOPER, Tennessee
PAUL A. GOSAR, Arizona	GERALD E. CONNOLLY, Virginia
PATRICK MEEHAN, Pennsylvania	JACKIE SPEIER, California
SCOTT DESJARLAIS, Tennessee	MATTHEW A. CARTWRIGHT, Pennsylvania
TREY GOWDY, South Carolina	TAMMY DUCKWORTH, Illinois
BLAKE FARENTHOLD, Texas	ROBIN L. KELLY, Illinois
DOC HASTINGS, Washington	DANNY K. DAVIS, Illinois
CYNTHIA M. LUMMIS, Wyoming	TONY CARDENAS, California
ROB WOODALL, Georgia	STEVEN A. HORSFORD, Nevada
THOMAS MASSIE, Kentucky	MICHELLE LUJAN GRISHAM, New Mexico
DOUG COLLINS, Georgia	<i>Vacancy</i>
MARK MEADOWS, North Carolina	
KERRY L. BENTIVOLIO, Michigan	
RON DeSANTIS, Florida	

LAWRENCE J. BRADY, *Staff Director*

JOHN D. CUADERES, *Deputy Staff Director*

STEPHEN CASTOR, *General Counsel*

LINDA A. GOOD, *Chief Clerk*

DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON FEDERAL WORKFORCE, U.S. POSTAL SERVICE AND THE CENSUS

BLAKE FARENTHOLD, Texas, *Chairman*

TIM WALBERG, Michigan	STEPHEN F. LYNCH, Massachusetts,
TREY GOWDY, South Carolina	<i>Ranking Minority Member</i>
DOUG COLLINS, Georgia	ELEANOR HOLMES NORTON, District of
RON DeSANTIS, Florida	Columbia
	WM. LACY CLAY, Missouri

CONTENTS

Hearing held on November 19, 2014	Page 1
WITNESSES	
Mr. Randy S. Miskanic, Vice President of Secure Digital Solutions, United States Postal Service	
Oral Statement	5
Written Statement	8
Mr. Guy J. Cottrell, Chief Postal Inspector, United States Postal Service	
Oral Statement	18
Written Statement	20
Ms. Tammy Whitcomb, Deputy Inspector General, United States Postal Service	
Oral Statement	28
Written Statement	30
Mr. Timothy H. Edgar, Visiting Fellow, Watson Institute for International Studies, Brown University	
Oral Statement	35
Written Statement	37
Mr. Charles E. Hamby II, Captain, Narcotic Enforcement Division, Prince George's County Police Department	
Oral Statement	49
Written Statement	51
APPENDIX	
Letters to DEI requesting hearings, submitted by Mr. Cummings	72
Answers to QFRs from Rep. Connolly to Tammy Whitcomb, USPS OIG	84
Answers to QFRs from Rep. Connolly to Guy Cottrell, USPS	92
Answers to QFRs from Rep. Connolly to Timothy Edgar, Brown University	102

EXAMINING DATA SECURITY AT THE UNITED STATES POSTAL SERVICE

Wednesday, November 19, 2014,

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FEDERAL WORKFORCE, U.S. POSTAL
SERVICE AND THE CENSUS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 11:40 a.m., in room 2154, Rayburn House Office Building, Hon. Blake Farenthold (chairman of the subcommittee) presiding.

Present: Representatives Farenthold, Walberg, Lynch, Clay, and Cummings.

Also present: Representative Davis.

Staff present: Melissa Beaumont, Majority Assistant Clerk; Will L. Boyington, Majority Deputy Press Secretary; Molly Boyd, Majority Deputy General Counsel and Parliamentarian; Adam P. Fromm, Majority Director of Member Services and Committee Operations; Jeffrey Post, Majority Senior Professional Staff Member; Laura L. Rush, Majority Deputy Chief Clerk; Andrew Shult, Majority Deputy Digital Director; Sarah Vance, Majority Assistant Clerk; Jaron Bourke, Minority Administrative Director; Marianna Boyd, Minority Counsel; Aryele Bradford, Minority Counsel; Jennifer Hoffman, Minority Communications Director; Tim Lynch, Minority Counsel; Dave Rapallo, Minority Staff Director; Katie Teleky, Minority Staff Assistant.

Mr. FARENTHOLD. The subcommittee will come to order. It is an interesting day. We have Mr. Issa staring over my shoulder now and Mr. Hoffield looking at me from over here. The pictures have been rearranged.

Anyway, I would like to begin this hearing by stating the Oversight Committee's mission. We exist to secure two fundamental principles: first, Americans have the right to know that the money Washington takes from them is well spent and, second, Americans deserve an efficient, effective Government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights.

Our solemn responsibility is to hold the Government accountable to taxpayers, because taxpayers have a right to know what they get from their Government. We will work tirelessly in partnership with citizen watchdogs to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy. This is the mission of the Oversight and Government Reform Committee.

I will now recognize myself for a short opening Statement.

We have called this hearing today to talk about the Postal Service's mail covers program. As we will hear from our panel this morning, mail covers have a long-running history at the Postal Service as a way of helping law enforcement investigations. But they remain a concern for privacy advocates.

Today, the mail covers program is managed by the Postal Service Inspection Service. This is the law enforcement arm of the Postal Service and it manages all incoming requests, oversees data security, and ensures mail covers are properly executed.

A mail cover itself is a fairly simple thing; it is a record of all the information on the outside of a mail piece for classes of mail that are sealed against inspection. Mail covers can be requested either by the United States Postal Service Inspection Service or outside law enforcement agencies. This information is often transcribed by hand, usually by Postal Service supervisors, just before a mail piece is delivered.

A mail cover can consist only of a single package or can cover all mail going to and from an addressee for 30 days or more. The vast majority of the 49,000 mail covers issued for Fiscal Year 2013 were 1-day covers internally requested by the Postal Service as part of drug investigations. However, more than 6,000 mail covers were requested by outside law enforcement agencies and approved by the Postal Service, while nearly 3,000 multi-day mail covers were requested internally by the Inspection Service.

On its May 2014 audit report, the Postal Service Office of Inspector General uncovered a number of troubling facts regarding the management and oversight of external mail cover requests. Of the audited covers, 21 percent were not approved by authorized individuals and 13 percent were approved without adequate justification contained in the request.

Moreover, despite receiving more than 6,700 requests of mail covers in Fiscal Year 2013, the Inspection Service denied just 10. That is an approval rate of 99.85 percent. That is better than my server is up. This fact raises serious questions about the current management of the mail covers program.

We will hear testimony from a number of witnesses who will be able to share the significant law enforcement benefits that this program can bring, as well as the privacy risk posed by this program if it continues to be poorly managed. We will also have the opportunity to hear from both the Postal Inspection Service and the IG with updates as to how the problems identified with the audit report are being addressed.

In addition to our discussion of mail covers program, we will probably get into discussing the data breach the Postal Service announced on November 10th, 2014. With respect to that data breach, the Postal Service has confirmed that personally identifiable information for more than 800,000 current and former Postal Service employees, including their name, addresses, and Social Security numbers, have been compromised.

While I understand some information regarding this breach may be still sensitive in nature, it is my hope that we can have a discussion about how the breach occurred, the extent of the data lost, and, most importantly, what actions are being taken to mitigate the risk of a similar breach in the future.

On that note, I greatly appreciate the written testimony that will be presented by Mr. Miskanic today. His testimony provides a clear time line of events leading up to the November 10th announcement that before today had not been available.

With that, I would like to thank all of our witnesses for being here today and allow the ranking member, the gentleman from Massachusetts, Mr. Lynch, to make an opening Statement.

Mr. LYNCH. Thank you, Mr. Chairman.

First, I want to apologize for being tardy. We have elections going on in the Democratic caucus, as well as the Republican caucus.

Mr. FARENTHOLD. Hope you did well in whatever you ran for.

Mr. LYNCH. Well, they haven't counted the votes yet. But that is another story.

Mr. Chairman, thank you very much for holding this hearing; I appreciate that. I also want to thank the members of the panel for your willingness to help this committee with its work.

Through the mail covers process, law enforcement agencies may request that the Postal Service record information on the outside of a piece of mail to obtain evidence of a crime, locate fugitives, identify property, and to protect the national security. According to Federal regulations, however, the Postal Service may not open or inspect the contents of a sealed piece of mail without a Federal search warrant.

Importantly, the mail covers program can serve as a valuable investigative tool through which postal investigators and law enforcement officials can further their investigations into the abuse of our mail system for terrorists or other criminal activity. However, our constitutional commitment to individual privacy and due process requires that we conduct meaningful oversight of this program in order to ensure that it is not unnecessarily broad in scope. Toward this end, the Postal Service inspector general recently reported some program deficiencies.

The IG reported that the chief postal inspector should, these are recommendations, No. 1, improve controls to ensure that responsible Postal Inspection Service personnel process the mail covers program as required; and, No. 2, the IG recommended that the Postal Service establish procedures to ensure periodic reviews of mail covers and that those are conducted as required; third, the Service recommended that we improve controls to ensure Postal Service facility personnel processes mail covers in a timely manner; and also, fourth, to implement system controls to ensure that data integrity in the Postal Inspection Service mail covers application.

The Postal Service has agreed with these recommendations and has fully implemented recommendation No. 2, establishing periodic review procedures. The agency has also made substantial progress on implementing the other three recommendations. Chief Inspector Cottrell expects all of the recommendations to be fully implemented by June 2015, so we will keep a watch on that.

On October 27, 2014, the New York Times published a story asserting that the mail covers program was more extensive than had been previously reported. In response, the Postal Service has reported to committee staff that the increase in mail covers was largely due to a change in accounting practices, which is easily un-

derstandable once the details are revealed. According to the Postal Service, starting in 2012, the Inspection Service began using 1-day mail covers on each individual piece of mail that the law enforcement agencies requested. Previously, a single mail cover could reflect Postal Service monitoring of multiple pieces of mail. So, naturally, this change in practice resulted in an increase in the number of total mail covers without necessarily reflecting an increase in the use of the mail covers program.

According to Chief Cottrell's testimony, there has been a reduction in the total number of mail covers used by law enforcement agencies over the past several years, and I look forward to hearing the details of these changes and surrounding each of the inspector general's recommendations.

On November 10th, 2014, the Postal Service publicly announced that its computer networks had been significantly breached. Personally identifiable information of his employees may have been compromised, including names, addresses, dates of birth, Social Security numbers, dates of employment, and other information. News reports indicate over 800,000 employees could be affected. This data breach comes on the heels of several other attacks in both the public and private sector, including Home Depot, Kmart, Target, JP Morgan Chase, USIS, the Community Health Partners, and most recently the U.S. State Department.

On November 10th, Ranking Member Cummings sent a letter to Postmaster General Donahoe requesting additional information about the breach, including the extent of the cyber attack, the nature of the data that was breached, and the number of potential employees and customers affected, and the Postal Service notification process regarding the breach. The ranking member also highlighted the need for greater collaboration to improve data security in light of the increased numbers of public and private data sector breaches.

I look forward to hearing from the Postal Service especially on the data breach piece of this, and how it plans to address the specific data security issues raised by the postal data breach and ensure that its employees and consumers are protected from such breaches in the future.

Thank you, Mr. Chairman. I yield back.

Mr. FARENTHOLD. Thank you, Mr. Lynch.

Other members will have 7 days to submit opening Statements for the record.

Mr. LYNCH. Mr. Chairman? I am sorry, I forgot. I would ask unanimous consent that Mr. Davis, the gentleman from Illinois, be allowed to participate. Mr. Davis is a former chairman of this subcommittee and has been a strong and eloquent advocate on behalf of postal employees and the postal system.

Mr. FARENTHOLD. Without objection, it will be an honor to let him join us today.

Mr. DAVIS. Thank you, Mr. Chairman.

Mr. FARENTHOLD. All right, our panel today, distinguished panel, Mr. Randy Miskanic is Vice President of Secure Digital Solutions for the United States Postal Service. Welcome, sir.

Mr. Guy Cottrell is the Chief Postal Inspector for the United States Postal Service Inspection Service. Welcome to you as well.

Ms. Tammy Whitcomb is Deputy Inspector General for the United States Postal Service Office of Inspector General. Welcome, ma'am.

Mr. Tim Edgar is Visiting Fellow at the Watson Institute for International Studies at Brown University. Go Bears.

Mr. Charles Hamby is a Captain with the Narcotics Enforcement Division of the Prince George's County, Maryland Police Department. Captain, a privilege to have you in front of us, as well, today.

Pursuant to the committee rules, we ask that all witnesses be sworn in before they testify. Would you all please rise? And if you will raise your right hand. Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

[Witnesses respond in the affirmative.]

Mr. FARENTHOLD. Let the record reflect that all witnesses have answered in the affirmative.

You all may be seated now.

We have had you all submit written testimony, so in order to allow us time to ask you questions, we ask that you summarize your testimony in 5 minutes or less. You will see in front of you a little timer. Green means go, yellow means hurry up, and red means stop.

So we will start with Mr. Miskanic. You are recognized for your summary of your testimony.

WITNESS STATEMENTS

STATEMENT OF RANDY S. MISKANIC

Mr. MISKANIC. Good morning, Chairman Farenthold, Ranking Member Lynch, and members of the subcommittee. Thank you for calling this hearing on data security at the Postal Service.

My name is Randy Miskanic and I serve as Vice President of the Secure Digital Solutions Group for the United States Postal Service. In this role I lead the Postal Service's digital product development initiatives. I am also a postal inspector, and I previously served as the Deputy Chief Inspector of the United States Postal Inspection Service. My experience as Deputy Chief included leading cyber investigations. Given this experience, the postmaster general appointed me to the role of Incident Commander in response to the cyber intrusion that became public last week.

On September 11th, the Postal Service Office of Inspector General was notified by US-CERT regarding four Postal Service servers that were sending unauthorized communication outside of the organization, indicating that these systems may have been compromised. On that date, we had limited information about the nature of the activity and we began a forensic investigation.

During the next several weeks, OIG agents and postal inspectors configured and installed the technical architecture and tools necessary to identify impacted servers and workstations on the Postal Service network.

By October 17th, it became apparent that the intrusion was very sophisticated and had been developed specifically to exploit the Postal Service computing environment. As the scale and the scope of the intrusion became evident, we greatly escalated our response.

We also worked closely with US-CERT, the FBI, and other forensic experts to develop a strategy for protecting our information systems.

By November 4th we were able to confirm that a compromised employee data set had been copied and removed from our network. This confirmation triggered our decision to quickly notify our employees.

Throughout this process, our guiding principles were to protect our information systems from additional harm, to ensure our employees' and customer data was secure, and to allow the investigation to proceed unnoticed by our adversary. One of our biggest challenges was maintaining secrecy regarding the remediation of our infected systems.

During the course of the investigative efforts, we learned of the sophisticated nature of the adversary and the dynamic tactics they employ to evade detection by most commercial information security tools. I can't get into too much detail about our processes except to say that it was critically important that the adversary not know that we were watching their activity. Any premature leak about our remediation steps might have caused this adversary to cover their tracks or take countermeasures that might have further harmed our network.

Over the weekend of November 8th and 9th, the Postal Service took a number of remediation steps that required shutting down and then restoring certain systems. Immediately afterward, on Monday, the 10th, the Postal Service notified its employees, customers, business partners, and other stakeholders about the intrusion. This occurred roughly 1 week after confirming the contents of the stolen employee data.

The compromised data included employee personally identifiable information. Additionally, customer call center data was also compromised. To date, we have seen no evidence that the compromised employee data has been used for malicious purposes such as identity theft. In an abundance of caution, however, the Postal Service is providing a 1-year creditor monitoring product at no cost to its employees, in addition to other services.

Mr. Chairman, the Postal Service operates one of the largest computer environments in the Federal Government. Until this recent intrusion, we have been successful in maintaining the integrity of our data and the security of our systems. Since being notified of the suspicious activity, the Postal Service has been engaged in a very intense process of evaluating and developing new strategies to protect our information systems. In parallel to complex investigative activities, we developed and continue to implement a detailed mitigation plan to stop the compromise and protect the Postal Service network.

On November 10th, the postmaster general notified our employees about the compromised data and made a commitment to strengthen the security of our systems to match these sophisticated new threats. The Postal Service will be taking numerous steps over the coming months to improve processes and technologies to better protect against future intrusions.

We live in a world that requires perpetual vigilance and staying a step ahead of our adversaries. We are committed to doing so on behalf of our employees, our customers, and the American public. Thank you, Mr. Chairman. This concludes my remarks.
[Prepared Statement of Mr. Miskanic follows:]



**STATEMENT OF
RANDY S. MISKANIC
VICE PRESIDENT, SECURE DIGITAL SOLUTIONS
U.S. POSTAL SERVICE
BEFORE THE
SUBCOMMITTEE ON FEDERAL WORKFORCE,
U.S. POSTAL SERVICE AND THE CENSUS
UNITED STATES HOUSE OF REPRESENTATIVES**

NOVEMBER 19, 2014

Good morning, Chairman Farenthold, Ranking Member Lynch, and members of the Subcommittee. Thank you, Chairman Farenthold for calling this hearing on Data Security at the Postal Service. My name is Randy S. Miskanic and I serve as Secure Digital Solutions Vice President of the United States Postal Service. In this role, I lead the Postal Service's digital product development initiatives with the goal of aligning our innovation strategy with customer demand for secure digital communications and experiences. I am also a Postal Inspector, and previously served as the Deputy Chief Inspector of the United States Postal Inspection Service (USPIS). The Postal Service and I are firmly committed to extending the trusted and secure aspects of the Postal Service brand into our digital innovations and future product offerings.

As the USPIS Deputy Chief Inspector, I led the USPIS's strategic approach to the prevention and investigation of identity theft and fraud offenses in the physical and digital arenas. During that time, I advanced the capability of the USPIS to conduct cyber investigations, respond to malware and network attacks and analyze digital evidence. I also guided the USPIS's efforts to build a robust cyber response and investigative capability through partnerships with the Carnegie Mellon University's Computer Emergency Response Team Coordination Center (CERT-CC) and other federal government and private sector partners.

With the discovery of the recent cyber intrusion into some of the Postal Service's information systems—an incident that has received broad media coverage—our Mass Data Compromise Response Plan (MDCRP) was invoked to ensure the appropriate level of technical, investigative and communications response. Given my prior experience in Secure Digital Solutions and in federal law enforcement, the Postmaster General appointed me to the role of Incident Commander to direct MDCRP activities.

I want to assure this subcommittee that protecting the privacy of customer and employee information is a priority for the Postal Service. The cyber security intrusion investigation, led by the Federal Bureau of Investigation (FBI) and joined by other federal and postal law enforcement and investigatory agencies, is ongoing.

The intrusion is limited in scope and nearly all operations of the Postal Service are functioning normally. Sadly, this incident is similar to a growing number of attacks reported by many other federal government entities and U.S. corporations. We are not aware of any evidence that potentially compromised customer or employee information has been used to engage in any malicious activity, and we are working with impacted individuals to mitigate potential misuse of such information.

Threat Assessment and Response Timeline

From the time we became aware of the potential threat to Postal Service information systems, our guiding principles were to protect our network from additional harm, to ensure our employee and customer data was secure, and to initiate an investigation that would not be detected by our adversary.

As our investigation of this incident progressed, it became apparent that the intrusion was very sophisticated and had been developed specifically to exploit the Postal Service computing environment. In fact, over the course of the investigation, we learned of the dynamic tactics employed by the adversary to evade detection by most commercial information security tools.

As the scale and scope of the intrusion became evident, we greatly escalated our response. One of our biggest challenges was maintaining secrecy regarding the remediation of several of our infected systems. Therefore, we worked closely with the U.S. Computer Emergency Readiness Team (US-CERT), the FBI and other forensic experts to develop a strategy for protecting our network.

Following is a high-level timeline of how the Postal Service learned of, investigated, mitigated and communicated the threat. I believe that you will find this timeline clearly reflects how—upon discovery that some of our information systems had been intruded—the Postal Service responded quickly and collaboratively, following the advice and guidance of federal and private sector cyber security experts.

Initial Discovery and Investigation

On September 11, 2014, the U.S. Postal Service Office of Inspector General (USPS OIG) reported that they received information from the US-CERT regarding four Postal Service servers that were sending unauthorized communication outside of the organization, indicating that these systems may have been compromised. Limited details were provided by US-CERT at that time.

During the period of September 12 through September 16, the USPS OIG alerted the Postal Service's Corporate Information Security Officer (CISO) of the suspicious network activity. The CISO was advised that the investigation should remain confidential. Furthermore, the USPS OIG provided the CISO with an operational security warning advising that actions taken without coordination are likely to adversely impact the Postal Service's overall security posture. The guidance document instructed the CISO to take no action – including further investigative

activity, scanning, re-imaging, resetting account passwords, taking systems offline or searching IP addresses.

The guidance provided by the USPS OIG was consistent with subsequent direction received from US-CERT and other agencies who have been engaged with these types of actors. The Postal Service's Chief Information Officer (CIO) was also subsequently notified of the threat during this period, and received the same security and operational warnings.

From September 16 through September 19, USPS OIG agents, Postal Inspectors, and members of the CISO team met daily to develop the steps necessary to properly investigate the suspected unauthorized network activity. Members of the investigative team performed forensic imaging and installed monitoring devices on servers suspected of being compromised. At this point all that was known is that four servers were sending unauthorized communications.

On September 19, the Postal Service CIO reported the suspicious network activity to the Postmaster General (PMG). The PMG was also advised at that time that the cyber intrusion investigation was ongoing and that only the USPS OIG and USPIS should take action to mitigate the threat and that any premature action could further endanger the network. Subsequently, information regarding this incident remained highly confidential and restricted to only individuals directly involved with the investigation.

During the period of September 19 through October 2, USPS OIG agents and Postal Inspectors configured and installed the technical architecture and tools necessary to identify any impacted servers and workstations on the Postal Service network. These investigative actions resulted in the identification of three Postal Service user accounts and an additional 29 servers with indicators of compromise. Due to the broadening scope of compromise and resulting forensic analysis requirements, data was submitted to the U.S. Department of Defense Cyber Crime Center for forensic analysis.

On October 7, following five days of investigation that revealed suspicious remote communications emanating from several of the compromised machines, the USPS OIG and USPIS team learned that a large data file had been copied and removed from the Postal Service network. This file, however, was encrypted, limiting the ability of the investigative team to identify the data contained within. It was suspected that the file was copied to another server outside of the USPS network that was being controlled by an adversary. Extensive investigative efforts continued over the following days in an attempt to identify the content and location of the removed file.

On the evening of October 10, the CIO informed the PMG of the confirmed data exfiltration. The following day, the USPS OIG held a briefing with senior postal leadership to advise them of the incident and to develop a further course of action. It was decided that private sector experts specializing in computer intrusion and incident response would be sought to engage in the investigation and support mitigation planning.

From October 11 through October 15, USPS OIG agents and Postal Inspectors continued to monitor network traffic for additional compromised servers and workstations. During this period, USPS OIG agents conducted a forensic examination of the server containing the encrypted files. The ongoing investigation revealed that the adversary may have accessed and copied a Postal Service Human Resources file containing employee personally identifiable information (PII).

Mass Data Compromise Response Plan Invoked

On October 16, the PMG and postal leadership were advised by USPS OIG investigators of the suspected contents of the exfiltrated file. The investigators cautioned, however, that further extensive and complex forensic analysis was necessary to determine if the file actually contained PII.

The Postal Service CIO concurrently invoked the MDCRP—declaring that the critical incident would be managed through a formal Incident Command structure. As the appointed Incident Commander, I subsequently formed teams to handle various aspects of the plan—specifically, Technical Branch, Communications Branch and Investigative Branch teams.

The Technical Branch was charged with developing the remediation and mitigation strategy, along with assisting in the overall ongoing investigation. The Postal Service Information Technology (IT) Team was assembled under this Branch and immediately began working with US-CERT to determine more detailed information about the threat. This Branch also began consulting with Carnegie Mellon University's CERT-Coordination Center (CERT-CC), Microsoft Corporation, and other commercial firms specializing in computer intrusion incident response, network monitoring, and remediation strategies to assess the adversary's capabilities and tactics. These partners were also involved with evaluating the protection of critical Postal Service cyber assets.

The MDCRP Communications Branch was tasked with developing a strategy to communicate the ongoing incident to necessary stakeholders, and to develop a comprehensive internal and external communications plan. A critical component that was discussed extensively and thoughtfully planned, was content and timing of employee messaging in the event that the suspected loss of PII data was confirmed. Strategic business partner and public notification were also critical communications elements that required extensive planning efforts.

The MDCRP Investigative Branch was bolstered by additional resources and assigned specific actions to identify the scope of compromise, along with the impact on Postal Service data systems. A strategic and tactical support request was submitted to the FBI. In response, the FBI provided cyber security intrusion experts, communication support for stakeholder and public outreach, and introductions to executive contacts within other intelligence agencies.

On October 17, the FBI Cyber Unit provided a Top Secret/Sensitive Compartmented Information briefing to the Postal Service Incident Command leadership and advised that the adversary was

very sophisticated and that implementing mitigation activities or communicating the threat to employees or the public at that point could result in the threat being further embedded into the Postal Service network. The FBI also reemphasized the need to exercise a high level of operational security during the management of this critical incident.

During the following week, USPS OIG agents and Postal Inspectors continued to obtain forensic images and established network monitoring across the entire Postal Service organization.

Administration and Congressional Notification

On October 20, the Incident Command staff provided a classified briefing to the White House Cyber Security Director and National Security Council staff. The White House Cyber Security Director was instrumental in aligning the Postal Service with the appropriate Federal resources to assist with all facets of managing the critical incident.

On October 22, the Deputy Postmaster General, U.S. Postal Service Inspector General, Chief Postal Inspector and I conducted separate classified briefings for House Oversight and Government Reform Committee and Senate Homeland Security and Governmental Affairs Committee staffs. The Committee staffs were informed of the current status of critical incident activities, the proposed plan to implement remediation within the Postal Service network, and the suspected compromise of employee PII data.

Also on October 22, USPS OIG agents learned that forensically recovered employee data appeared to originate from the Postal Service Human Resources Shared Service Center, however, contents of the encrypted files were still not known.

Communications Planning Intensifies

On October 23, the MDCRP Communications Branch team began working with select internal Postal Service department representatives to develop action plans for communicating with stakeholders during a hypothetical incident in which employee PII was accessed by an external entity. While it was still unknown at that time if employee PII had in fact been taken, all department representatives were required to plan for this scenario during a series of confidential meetings. As a result of the follow-up exercises, pertinent areas of focus, necessary tasks, and services required to assist potential victims were identified.

A significant challenge in developing communications that would provide the necessary information and details regarding available assistance, was that the contents of the compromised data was unknown for much of the time between discovery and announcement. As the technical analysis of the intrusion identified the scope of the breach, we tailored messaging to ensure all affected victims would be provided with the information necessary to assist in protecting them from the consequences of any illegal use of the compromised data.

Timing of public communication was also a serious concern. From the technical perspective, experts within the Postal Service and from supporting agencies provided prudent warnings that short-term remediation efforts would be seriously compromised if the threat actor became aware that the intrusion had been discovered. If provided advance warning of network actions intended to expel and block the intruder from the Postal Service network, the adversary could take bolder steps to further infiltrate or sabotage systems. This valid threat of additional potential damage to the Postal Service and victims was deemed sufficient basis to delay notification and public announcement until after short-term remediation was accomplished.

Another concern focused on the needs of the victims of this network intrusion. In similar data breaches within other organizations, potential victims attempted to reach support services, such as credit monitoring, before those services were in place and ready to assist. We sought to avoid any additional frustration for our employees and affected customers, and we worked with our credit monitoring vendor to ensure victims would be able to access services in a timely manner.

An inability to effectively answer employee, customer, and business partner questions regarding the specific content and victims of the compromised data created yet another concern. Prematurely announcing the intrusions before these important facts were discovered would have undoubtedly led to a great deal of frustration and confusion.

US-CERT Engagement Increases

On October 23, US-CERT officials also briefed postal leadership and Incident Command staff about the type of adversary likely responsible for the intrusion. The officials also reinforced FBI guidance regarding operational security practices, cautioning against public notice and mitigation actions being taken too soon.

The US-CERT Director provided critical strategic advice regarding the scope, phases and duration of activities associated with the deployment of the remediation plan. Additionally, the Director cautioned that the Postal Service was moving very aggressively and an improperly resourced plan could alert the adversary, which could then open the Postal Service network to deeper penetration and make eliminating unauthorized access more difficult.

From October 26 through October 28, the forensically recovered employee PII data from the compromised server was reconstructed and shared with the Postal Service Chief Human Resources Officer (CHRO). The investigative team subsequently confirmed through detailed forensic mapping and analysis that the recovered Postal Service employee PII was indeed compromised by the adversary. Review of additional forensic evidence indicated that files were extracted to a server outside of the Postal Service network, albeit the investigative team still did not know what, if any, files actually were stolen.

On October 31, the investigative team identified a database backup file on a compromised server, which was determined to be related to an application used for receiving, processing and

managing customer service requests. The database backup file was located on a compromised server that was determined to have 2.9 million customer complaints. The compromised customer data was limited to name, address, phone and email address information provided in the course of each customer complaint.

Data Compromise Confirmed and Remediation Plan Activated

On November 4, the investigative team—with the assistance of US-CERT—confirmed that the Postal Service employee PII data was copied and stolen from the Postal Service network. The scope of the compromised data included, names, dates of birth, social security numbers, addresses, beginning and end dates of employment, emergency contact and other information. The following day, the Postal Service received mitigation recommendations from US-CERT to successfully evict the adversary from the Postal Service network.

On November 7, the Postal Service CIO organization activated a remediation plan developed with US-CERT guidance and supported by external cyber security experts. Implementing remediation plan elements required initiation of an information systems network brownout period, which limited communications between the Postal Service network and the Internet.

Also on November 7, the Deputy Postmaster General, Chief Postal Inspector and I also conducted a joint briefing for House Oversight and Government Reform Committee and Senate Homeland Security and Governmental Affairs Committee staffs regarding the timing of our remediation plans and employee and public notifications.

During the November 8 – November 9 brownout period, virtual private network (VPN) connections were blocked and remote network access was denied. Sending and receiving email messages between Postal Service email accounts was allowed during the brownout, however, sending and receiving emails messages between postal accounts and non-postal accounts was blocked. The brownout did not affect mail collection, processing, and delivery operations. In addition, retail, usps.com, and employee and customer-facing applications functioned normally during this period.

The new network security safeguards put into place over this two-day period included removing workstation administrator rights and enhancing network monitoring. We also upgraded and segmented Administrative Domain Controllers, removed compromised systems and accounts, and implemented two-factor authentication for administrative accounts.

To further reduce the likelihood of phishing or spear-phishing emails—common and increasingly sophisticated ways of compromising computer users and systems—impacting the Postal Service network, access to personal email sites such as Gmail or Yahoo was, and continues to be, blocked. In addition, direct database access is now only enabled to technology support staff and a number of business applications have been retired. These safeguards will continue to be reviewed and enhanced over the coming months in order to increase our overall security posture.

Comprehensive Communications Plan Activated

With the confirmation that employee PII had actually been compromised, and completion of initial remediation efforts, the Postal Service quickly activated its comprehensive communications plan developed for this incident.

The PMG recorded a video to be used in conjunction with other messaging for the purpose of informing employees of the intrusion and remediation activities. Postal managers were provided prepared materials and instructed on how employee communications materials should be disseminated. In addition to the PMG video, prepared materials included hardcopy versions of mandatory employee stand-up talks, anticipated questions and answers, and talking points for communicating with customers. These materials were also posted to the Postal Service's intranet site. In addition, messaging on the cyber intrusion was included in the daily electronic newsletter delivered via email to all employees with computer access, and notices were posted on employee bulletin boards.

Key postal stakeholders, including Union and Management Association national presidents, strategic business partners, including mailing industry leaders, and heads of key federal agencies were personally contacted and informed of the security breach. The Administration, House and Senate Leadership and Congressional Oversight Committee members were also informed that public messaging of the cyber intrusion was beginning. Electronic newsletters delivered information to subscribing customers. Customer information about the intrusion, including a fact sheet and anticipated questions and answers, were also posted on usps.com and other postal customer-facing websites.

Customer Impacts of Cyber Intrusion

At this time, we do not believe that Postal Service transactional revenue systems in Post Offices, as well as on usps.com where customers pay for services with credit and debit cards, were affected by this incident. There is no evidence that any customer credit card information from retail or online purchases, change of address or other services was compromised. Postal Service operations were not impacted by the breach – Post Offices are functioning normally and mail and packages are being delivered as usual.

As noted earlier in my testimony, the intrusion did compromise data submitted by customers who contacted the Postal Service Customer Care Center with an inquiry via telephone or e-mail. For customers who provided such information between January 1, 2014, and August 16, 2014, this data consists of names, addresses, telephone numbers, email addresses and other information. The Postal Service does not believe that these potentially affected customers need to take any action as a result of this incident. While we are aware of no evidence that would suggest that credit monitoring is needed at this time, we are continuing to investigate and will of course provide such monitoring if it is deemed appropriate.

Employee Impacts of Cyber Intrusion

The investigation indicates that all 800,000 plus Postal Service career and non-career employees nationwide, including those working for the Postal Regulatory Commission, the Office of Inspector General and the U.S. Postal Inspection Service, have been affected by the breach. No beneficiary information was compromised, and the incident did not affect Postal Credit Unions or Thrift Savings Plan accounts. Compromised files may also have included PII for employees who left the organization anytime from May 2012 to the present. We are additionally aware of a possible compromise of injury compensation claims data that we are still investigating.

The Postal Service is making credit monitoring service available to all employees, as well as those who left the organization since May 2012, at no charge for one year. Last week, letters were sent to employees advising them of the compromised PII data and provided a unique activation code to enroll in the service within 90 days of the date of the letter. All employees are encouraged to take advantage of this service.

While we are not aware of any evidence that any of the compromised employee information has been used to engage in any malicious activity, the credit monitoring service is being offered out of an abundance of caution. Postal Service forensic investigators are conducting a thorough review of the affected databases and if the ongoing investigation determines that any additional employee information has been compromised, employees will be notified. Postal employees, like everyone else, are advised to keep vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring credit reports.

Next Steps

The privacy and security of data entrusted to the Postal Service is of the utmost importance. Our entire leadership team is committed to taking the steps necessary to prevent a cyber security intrusion from happening again.

During the activation of our remediation plan, Carnegie Mellon's CERT-CC performed a vulnerability assessment on systems that were compromised. The team evaluated both processes and technical security controls. The assessment included scanning and penetration testing of select human resource systems, review of vulnerability scans for select systems, interviews with system owners, and review of general security policies related to authentication, system hardening, and perimeter defenses.

CERT-CC found that the Postal Service has solid policies for information security; however, various business units do not always follow these policies. It also found that critical systems could be protected by better segregation from the general IT user systems. Starting with security measures that we put in place as soon as we confirmed that employee PII was compromised, we are continuing to institute numerous additional measures designed to improve the security of our information systems. One such future change includes requiring employees

to complete two-factor authentication to access individual user accounts and some applications. Additionally, we plan to request assistance from CERT-CC to conduct a full-scope vulnerability and penetration test of our network.

Going forward, the Postal Service will also increase our collaboration with government agency partners such as US-CERT and the National Cybersecurity and Communications Integration Center (NCCIC) to understand tactics used by cyber security adversaries, as well as other threats to national security. Additionally, we will continue to improve our security posture in line with US-CERT recommendations, which include increasing network monitoring, increasing network segmentation, improving user management controls, improving server security controls, thus improving our overall information security posture. These improvements will require the procurement of new hardware and information security services.

The Postal Inspection Service also will join the National Cyber Investigative Joint Task Force (NCIJTF). Membership in this task force will enhance the ability of the USPIS to proactively act upon intelligence information and learn more about evolving threats. In addition, Postal Inspectors will be better positioned to coordinate, integrate, and share information related to cyber threat investigations.

Conclusion

The Postal Service takes its responsibility to safeguard the personal information of our customers and employees very seriously. No company or organization connected to the Internet is immune from the type of malicious cyber activity that the Postal Service experienced. We take such threats seriously and regularly take action to protect our networks, our customers' data, and our employees' information.

As a result of this incident, we have significantly strengthened our systems against future cyber intrusions. We will continue taking all necessary steps to guard our systems from attacks and to ensure the safety and privacy of our employees and customers. Thank you, Mr. Chairman, for the opportunity to submit this testimony. I welcome any questions that you and the Committee members may have.

###

Mr. FARENTHOLD. Thank you very much. I look forward to questioning you.

Mr. Cottrell, you are up.

STATEMENT OF GUY J. COTTRELL

Mr. COTTRELL. Good morning, Chairman Farenthold, Ranking Member Lynch, and members of this subcommittee. I am Guy Cottrell, Chief Postal Inspector of the United States Postal Service. On behalf of the men and women of our agency, I appreciate this opportunity to present the testimony of the U.S. Postal Inspection Service in support of this hearing on data security at the U.S. Postal Service.

My testimony today will discuss the Postal Service mail cover program and the controls in place to ensure appropriate privacy protections are maintained. I will also update the committee on the progress made regarding recommendations contained in the Postal Service Office of Inspector General Report released in May 2014 on the mail cover program.

The Postal Service respects the privacy of its customers and the sanctity of the mail. A mail cover is the process by which a non-consensual recording is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter. Any personal information obtained in connection with the mail cover program is treated as restricted, confidential information and is not publicly available.

Over the past 5 years, law enforcement use of mail covers has generally declined, with one significant exception. We revised procedures in connection with criminal investigations into dangerous mail and narcotics in Fiscal Year 2012. These programs emphasized the safety of postal employees and strive to protect them from handling mail that contains harmful substances, narcotics, and trafficking proceeds, and the violence associated with drug crimes.

Equally important, they aid our efforts to help keep illegal drugs off the streets and out of school yards across the Country. We now assign mail covers to individual mail pieces in these investigations, which drove the spike in overall mail cover volume the last three fiscal years.

Recently, the Postal Service inspector general conducted its review of the mail cover process, releasing a report in May 2014 containing four recommendations to improve program security and accountability. We have addressed these recommendations as follows:

We have worked to improve controls to ensure responsible Postal Inspector Service personnel process mail covers as required.

We have examined the administration of the program and our processes, updating standard operating procedures, improving training, testing application workflow enhancements, creating performance metrics, and formulating a disbarment process.

We have established procedures to ensure periodic reviews of the mail cover program are conducted at national headquarters and in the field as part of our annual compliance review process.

We are leveraging existing Postal Service tools to better assess program compliance at the local post office level and facilitate communication.

We have also initiated a project to upgrade the mail cover process, allowing us to better ensure data integrity, compliance, and accurate reporting.

We are on target to completely address all audit recommendations by June 2015.

I am certain these actions will provide necessary safeguards to ensure the program is administered as required.

Recent media coverage has confused three independent mail programs, the mail cover program, mail imaging, and mail isolation control and tracking, or MICT, creating a false impression that there is a vast mail monitoring system in operation. This simply is not true. These programs are distinct and have very different purposes.

I have already discussed the mail cover program. Mail imaging was developed in the early 1990's to help automate mail processing. The images are not maintained in a centralized data base, not profiled for mailing habits, nor are they mined or analyzed electronically.

Mail isolation control and tracking, MICT, is a set of safety procedures developed in response to the anthrax mailings of 2001, and it is triggered when a potentially contaminated mail piece is identified to help determine potential contamination of mail processing equipment, facilities, and vehicles. Safety is the ultimate goal of MICT, although the contamination path can be relevant for law enforcement purposes.

In closing, I would like to thank the committee for inviting me to appear here today to discuss with you our commitment to strengthening the mail cover process, allowing us an opportunity to better explain our use of this important investigative tool and the safeguards in place to protect the privacy of the American public.

Thank you, Mr. Chairman.

[Prepared Statement of Mr. Cottrell follows:]



**STATEMENT OF
GUY J. COTTRELL
CHIEF POSTAL INSPECTOR, U.S. POSTAL SERVICE
BEFORE THE
SUBCOMMITTEE ON FEDERAL WORKFORCE,
U.S. POSTAL SERVICE AND THE CENSUS
UNITED STATES HOUSE OF REPRESENTATIVES**

NOVEMBER 19, 2014

Chairman Farenthold, Ranking Member Lynch, and members of this subcommittee, I am Guy J. Cottrell, Chief Postal Inspector of the U.S. Postal Service. On behalf of the men and women of our agency, I appreciate the opportunity to present the testimony of the U.S. Postal Inspection Service in support of this hearing on Data Security at the U.S. Postal Service.

As one of our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, we have a long, proud, and successful history of fighting crime against those who attack our nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public. For over 250 years, Postal Inspectors have investigated criminal offenses involving the mail and the postal system. From embezzlements in colonial Post Offices to mail train robberies in the 1800s, from major fraud cases in the 1900s to the mailing of deadly anthrax in 2001, Postal Inspectors have worked diligently to ensure America's confidence in the U.S. Mail.

Postal Inspectors tenaciously investigate criminal offenses involving the mail or the postal system. As federal law enforcement officers we carry firearms, make arrests, and serve federal search warrants and subpoenas. To carry out our mission, Inspectors work closely with the Department of Justice and U.S. Attorney's Offices, other federal and local law enforcement agencies, and local prosecutors to investigate cases and prepare them for court. Postal Inspectors enforce more than 200 federal laws related to crimes that fraudulently use or adversely affect the U.S. Mail, the postal system, postal employees and postal customers.

The Postal Inspection Service helps secure the nation's mail system and ensure public trust in the mail. This is accomplished through public awareness, prevention efforts, and the aggressive investigation of individuals who violate federal laws and Postal Service rules and regulations. To effectively enforce the law and enhance the security and privacy of the U.S. Mail, we have stationed approximately 1,400 Postal Inspectors throughout the United States and have a presence in Puerto Rico, Guam, the Virgin Islands and Germany, as well as at Universal Postal Union (UPU) Headquarters in Berne, Switzerland. In Fiscal Year (FY) 2013, these Inspectors initiated more than 8,200 cases, and reported 6,080 arrests and indictments along with 5,041

convictions.¹ They also responded to more than 3,400 incidents involving suspicious items, substances, powders or liquids in the mail or at postal facilities.

My testimony today will focus specifically on the Postal Service's mail cover program, and the controls in place to ensure appropriate privacy protections are maintained. I will also update the Committee on the progress made regarding recommendations contained in the Postal Service's Office of Inspector General's Report; "Postal Inspection Service Mail Covers Program" released in May 2014.

I would first like to take this opportunity to state for the record the definition of a mail cover. There has been a great deal of confusion in the public as of late, spurred primarily by erroneous media reports, concerning this investigative tool and its use.

A mail cover is the process by which a nonconsensual recording is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter (e.g., the name and address of the sender and addressee) or by which a record is made of the contents of any unsealed class of mail matter, for one of the following reasons:

- (i) To protect national security,
- (ii) To locate a fugitive,
- (iii) To obtain evidence regarding the commission or attempted commission of a crime, punishable by law by imprisonment for a term exceeding one year,
- (iv) To obtain evidence of a criminal violation or attempted criminal violation of a postal statute, or
- (v) To assist in the identification of property, proceeds or assets which are forfeitable because of a violation of criminal law.

The regulations governing mail covers are found at 39 CFR § 233.3. The regulations state the Postal Service maintains rigid control and supervision with respect to the use of mail covers as an investigative technique for law enforcement or the protection of national security. This function has been delegated to me in my position as the Chief Postal Inspector.

The Postal Service is committed to the privacy of customers. Any personal information obtained in connection with the mail cover program is protected in accordance with the Privacy Act. Information obtained from mail covers must be treated as restricted, confidential information. Inadvertent or intentional compromise of an investigation may result from someone informing the subject a mail cover is in effect or by revealing information obtained from a mail cover. Only postal personnel are authorized to record information relevant to mail covers and this information should only be disclosed at the express direction of the Postal Inspection Service for a law enforcement purpose as described above. Misuse or abuse of the mail cover process,

¹ Arrests, indictments, and convictions may be related to cases from prior reporting periods.

including improper disclosure of mail cover information, has resulted in disciplinary action of postal employees.²

Concerning the actual mail covers, however, courts have found there is no reasonable expectation of privacy with respect to information contained on the outside of mail matter. Courts have consistently upheld this principle and the constitutionality of Mail Covers in general, both prior³ to the Supreme Court's holding in *Katz v. United States*, 389 U.S. 347, as well as in subsequent decisions.⁴ No reasonable expectation of privacy exists which would otherwise be protected under the Fourth Amendment as a person has no legitimate expectation of privacy in the information voluntarily turned over to a third party. There is an obvious need for the Post Office to read and review information contained on the outside of a mail piece in order to ensure it reaches its destination. *United States v. Choate*, 576 F.2d 165, 175 (9th Cir. 1978). Of further note, courts have held a mail cover is substantially less intrusive than other law enforcement techniques. See *United States v. Gering*, 716 F.2d 615, 619-620 (9th Cir. 1983) (citing *Choate*).

It is important to note the lack of a reasonable expectation of privacy applies only to the information contained on the outside of the mail piece. Any information or matter contained within a mail article sealed against inspection remains subject to the protections of the 4th Amendment and the requirement of a Federal search warrant. Since 1878 it has been well settled that the 4th Amendment protects against the warrantless opening of sealed letters and packages in order to examine the contents. See *Choate*, 576 F.2d at 174 (citing *Ex parte Jackson*, 96 U.S. 727). The Postal regulations authorizing the use of mail covers were instituted the next year acknowledging the sanctity of the correspondence, but instituting the Postal Service's interpretation of the *Jackson* decision to allow mail covers. *Id.* at 177.

In 1965, Senator Edward Long, chair of the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, held hearings on invasions of privacy. The hearings looked at multiple agencies and their acquisition of information. A part of those hearings included the use of mail covers. In response to these hearings the Postmaster General issued new and more rigid regulations. Subsequent to the issuance of the regulations, Senator Long expressed satisfaction with the new regulations. See *Choate*, at 178.

To make the regulations regarding mail covers more accessible to the public and to discourage confusion regarding the nature of mail covers, the Postal Service republished the mail cover

² *Robert W. Holdsworth, Jr., Petitioner, v. United States Postal Service, Respondent*. 2011-3214, United States Court of Appeals for the Federal Circuit, 469 Fed. Appx. 871; 2012 U.S. App. LEXIS 2481. February 9, 2012. Decided. The court upheld an MSPB final decision which upheld the termination of a Postal Service letter carrier who informed a customer on his route that authorities were watching his mail.

³ *United States v. Costello*, 255 F.2d 876, 881 (2d Cir. 1958); *Canaday v. United States*, 354 F.2d 849 (8th Cir. 1966); *Cohen v. United States*, 378 F.2d 751 (9th Cir. 1967); *Lustiger v. United States*, 386 F.2d 132 (9th Cir. 1967).

⁴ *United States v. Balistrieri*, 403 F.2d 472, 475-477 (7th Cir. 1968); *United States v. Isaacs*, 347 F. Supp. 743, 750 (N.D. Ill. 1972), affirmed on other grounds, 493 F.2d 1124 (7th Cir. 1974); *United States v. Leonard*, 524 F.2d 1076, 1087 (2d Cir. 1975); *United States v. Bianco*, 534 F.2d 501, 508 (2d Cir. 1976); *United States v. Huie*, 593 F.2d 14 (5th Cir. 1979); *United States v. Choate*, 576 F.2d 165, 175 (9th Cir. 1978) (finding no violation under First, Fourth, and Ninth Amendment); *United States v. De Poli*, 628 F. 2d 779, 786 (2nd Cir. 1979); *Vreeken v. Davis*, 718 F.2d 343, 347 (10th Cir. 1983); *United States v. Gering*, 716 F.2d 615, (9th Cir. 1983) (finding no violation under the First and Fourth Amendment); *United States v. Hinton*, 222 F.3d 664, 675 (9th Cir. 2000)

regulations in the Federal Register 40 FR 11579 (1975) (codified in 39 CFR 233.2 and later re-designated 233.3 in 46 FR 34330 (1981)). The republication notes the use of mail covers has been governed by Section 233.2 (1971) of the Postal Service Manual with supplementation by provisions formerly contained in Part 861 (1965) of the Postal Manual of the old Post Office Department. The Federal Register updated provisions related to delegating authority but made no substantive changes in mail cover procedures or safeguards.

Mail covers may be used as an investigative tool by other law enforcement agencies, however, a written request must be made through the U.S. Postal Inspection Service. Requesting law enforcement agencies must treat mail covers as restricted and confidential information. As with internal mail cover requests outside law enforcement agencies must demonstrate reasonable grounds for requesting and using a mail cover. The requesting law enforcement agency must explain what criminal law the subject of the mail cover is violating and how the mail cover could further the investigation or provide evidence of a crime. Mail covers are authorized only when all requirements are met within the written request. The Postal Inspection Service reviews each request to ensure it contains enough information to stand alone, as full justification for the cover and fully complies with all regulation requirements. The Postal Inspection Service does not approve all submitted requests, declining both internal and external law enforcement mail cover requests for failing to meet program criteria.

Trends over the past five years indicate a continued reduction in the use of mail covers by outside law enforcement agencies. This trend is consistent with the decreased use of mail covers by the Postal Inspection Service, with one significant exception. In late FY 2012, the Postal Inspection Service revised procedures in connection with criminal investigations into dangerous mail and narcotics investigations. This procedural change, whereby we assigned mail covers to individual pieces of mail as opposed to an operation, drove the increase in the total mail cover number. For example, a mail operation at a postal facility in FY 2011 would have used a single mail cover. Today, the same operation would generate numerous one-day mail covers for mail pieces suspected of containing narcotics or narcotics proceeds. This procedural change resulted in the spike in mail covers as illustrated below:

Mail Covers by Category	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014
Inspector Mail Covers	3391	3195	3187	2848	2824
Outside Agency Mail Covers	9462	9233	8265	6732	6274
One-Day Mail Covers	4956	4327	4652	41102	48095
Total Mail Covers	17809	16755	16104	50682	57193
Mail Volume (Billions)	170.9	168.3	159.9	158.4	155.4

In comparison to volume of mail processed by the Postal Service, the number of mail covers requested and approved is miniscule.

The Postal Service Inspector General conducted its first review of the mail cover process, releasing its report in May 2014, entitled "Postal Inspection Service Mail Covers Program" (HR-

AR-14-001). At the committee's request, following is an update on the progress, to date, on actions outlined in our management response.

The Inspector General's first recommendation advised the Postal Service to improve controls to ensure responsible Postal Inspection Service personnel process mail covers as required. The Inspection Service has taken the following steps:

- Reviewed and updated standard operating procedures for administering the mail cover program, completed in FY 2014. A second review is scheduled for FY 2015;
- Updated program materials that outline policies and procedures for other law enforcement agency use of mail covers. A comprehensive review and overhaul of program materials will be completed in FY 2015;
- Developed performance metrics and management reports to record receipt of outside agency criminal mail cover requests and to ensure timely processing;
- Developed, and is now testing, system enhancements to track and follow-up on non-return of accountable documents by outside agencies. Additional testing, and process refinement is required;
- Piloted the use of existing USPS applications to notify postal facilities to complete mail covers and return accountable materials. This limited trial has improved response rates by 5 percent. We are expanding the trial, and are seeking methods to further increase the response rate, better improving the process before wide-scale implementation;
- Is developing an internal training guide which is in the final stages of development; and,
- Is developing a disbarment process to hold external law enforcement agencies accountable for non-return of accountable items.

Based on continued action necessary to ensure success on these initiatives, we have requested an extension of the target completion date to March 30, 2015.

The second recommendation advised the Postal Inspection Service to establish procedures to ensure periodic reviews of mail covers are conducted as required. The Inspection Service revised procedures for conducting periodic reviews of mail covers, which are incorporated into the annual comprehensive self-assessment process. Beginning FY 2015, all field divisions will review mail cover procedures as part of their assessment. Mail cover compliance items may also be reviewed as part of the on-site compliance review program, which is an additional on-site assessment performed by a headquarters compliance team, with each division undergoing on-site assessment on a three-year cycle. We consider action on this item complete, and have requested the Inspector General close-out the finding.

The Inspector General's third recommendation advised the Postal Service to ensure Postal Service facility personnel process mail covers in a timely manner. The Inspection Service has piloted an existing Postal Service tool as a method to assess and ensure compliance with mail cover operations. We have also piloted the application, as stated above, to help ensure mail covers are completed timely and materials returned as required. We have also developed reporting tools for postal managers to better communicate compliance in handling mail covers.

Additional tasks remain to be accomplished, however, to ensure the recommendation is fully addressed. We believe this can be achieved by March 30, 2015, and have requested the Inspector General establish the estimated completion date accordingly.

The Inspector General's fourth recommendation advised the Postal Service to implement system controls to ensure data integrity in the Postal Inspection Service mail cover application. The Postal Inspection Service is committed to ensuring data integrity, and immediately initiated a review of existing program scripts, with a commitment to enact modifications as necessary to ensure automated processes are functioning properly. These tasks are in progress. We have initiated a formal mail cover system upgrade project, with the objective to improve the overall mail cover application, ensuring data integrity, compliance, and accurate reporting. The target implementation was stated as June 30, 2015; work is in progress and on track to achieve this date.

The mail cover is an important investigative tool, and we welcomed the Inspector General's review of the mail cover process to help us safeguard its future use. I am certain these recommendations, along with the additional actions we are taking will continue to provide necessary safeguards to ensure the program is administered as required.

The mail cover has been in use, in some form, since the 1800's. Today, the most common use of this tool is related to investigations to rid the mail of illegal drugs and illegal drug proceeds. Our narcotics program emphasizes the safety of postal employees and strives to protect them from handling mail that contains narcotics and trafficking proceeds and the associated violence. To accomplish this goal our investigations target drug trafficking rings and parcels containing contraband. In FY 2013, the Postal Inspection Service seized more than 46,000 pounds of illegal narcotics and \$20.7 million in drug trafficking proceeds from the mail. These results are tied to investigations such as one in which Postal Inspectors arrested 12 suspects in California accused of shipping illegal drugs to college students. Inspectors seized more than 300 mailings containing approximately 80 kilograms of marijuana, hashish, and ecstasy, plus about \$50,000 in drug-related proceeds. Similarly, in another case which focused on drug trafficking rings using First-Class and Express Mail to ship methamphetamine from California to Guam, Inspectors obtained 321 federal search warrants, seized nearly 11 pounds of methamphetamine, and arrested 10 suspect traffickers.

I would also like to address the misconceptions surrounding the mail cover and its use by law enforcement.

- A mail cover is not used merely as a routine investigative tool.
- The Postal Service does not use its automated processing equipment to gather this information.
- Data obtained under a mail cover is collected through a manual process.
- The mail cover is not used as part of a surveillance strategy by the Postal Service to monitor the mailing behaviors of the American public.

The Postal Service respects the privacy of its customers and the sanctity of the mail. Contrary to recent media reports, the Postal Service does not monitor the mail of its customers and it does not maintain any system or program of "surveillance." Unfortunately, recent press coverage has conflated three independent mail programs—the mail cover program, mail imaging, and Mail Isolation, Control and Tracking (MICT). The result is a wholly false impression that there is a vast mail monitoring system in operation. This is simply not true.

These programs are distinct from one another and have very different purposes. Mail covers are used for criminal investigations, as previously explained.

Contrary to recent media assertions, mail imaging is not a "surveillance" tool – it is a mail processing tool. Mail imaging is a process developed by the Postal Service in the early 1990's that allowed for the automation of mail processing. Individual mail processing machines create images that make it possible for machines, rather than people, to sort mail, thereby reducing costs and increasing speed and accuracy of delivery. Of the 158 billion pieces of mail processed in FY 2013 by the Postal Service, fewer than 23 billion (less than 15 percent) were subjected to a process that generates a mail piece image that is stored for more than a brief period, up to seven days. Those images reside locally at the processing plant. They are not stored in a database, nor do they reside in a format that allows them to be mined or analyzed electronically.

Finally, Mail Isolation, Control and Tracking (MICT) is a set of safety procedures developed in response to the anthrax mailings that occurred in October of 2001. The purpose of these procedures is to protect Postal Service employees and the American public in the event a known contaminated piece of mail has been processed through postal equipment. MICT is only triggered when a potentially contaminated mail piece is identified, and the ultimate goal is to be able to trace the path of the contaminated mail piece through the mail processing system so that the facilities, vehicles and processing machines that came in contact with the mail piece can be isolated and appropriate safety measures can be taken. Generally, the tracking is accomplished by barcode information that is placed on the mail piece during processing. Once the path of a contaminated mail piece has been determined, appropriate safety measures can be taken. Safety is the ultimate goal of MICT, not "surveillance", although the path of a contaminated mail piece can be relevant for law enforcement purposes as well.

Tracking the path of a known contaminated mail piece is an investigative technique used by the Postal Inspection Service fewer than ten times in recent years. In one such case a mail piece containing ricin, addressed to the President of the United States, was identified in the mail stream before it could reach the President. This case, which received extensive national media attention, resulted in a successful prosecution and conviction, due in large part to the use of this valuable investigative technique.

In closing, I'd like to thank the committee for inviting me to appear here today. I appreciate the opportunity to discuss with you our commitment to strengthening the mail cover process; allowing us an opportunity to better explain our use of this important investigative tool, and the safeguards in place to protect the privacy of the American public. I also appreciate the

opportunity to address inaccurate reporting in the media regarding the mail cover process. Despite the continued decline in its use, the mail cover remains a valuable tool in the law enforcement community and the American public has nothing to fear from its use. Mail covers have long assisted our efforts to remove illegal drugs from the mail stream, keeping them off the streets and out of schools across the country. They have aided us in helping identify countless elderly victims who could ill-afford to lose their life savings to criminals who act without a conscience.

Over the past year media reports have conflated the use of mail covers, mail imaging, and the MICT process to suggest a conspiracy to spy on the mail of the American public—whom we are honored to serve and who trust us to keep the mail safe. This notion could not be further from the truth.

I welcome your questions.

Mr. FARENTHOLD. Thank you very much.
Ms. WHITCOMB.

STATEMENT OF TAMMY WHITCOMB

Ms. WHITCOMB. Mr. Chairman and members of the committee, thank you for the opportunity to discuss our recent audit report on mail covers.

Mail covers have been an investigative tool for more than 100 years, used for tracking financial frauds, drug trafficking, and other criminal activity. A mail cover involves postal officials recording the information from the outside of a mail piece, such as the sender's address. However, the mail cover program does not permit opening letters and packages that are sealed against inspection, as this requires a search warrant. To be clear, the program should not be confused with the operational imaging of mail pieces to manage mail flows.

The U.S. Postal Service processed approximately 49,000 mail covers in Fiscal Year 2013. Mail covers can be requested either by external investigators, including my office, or by the Postal Inspection Service. There are different types: mail covers that target individuals in suspected criminal matters, mail covers that target postal facilities where mail and parcels associated with criminal activity are passing, and special mail covers used for national security purposes.

The OIG is responsible for auditing the investigative activities of the Postal Inspection Service. As part of this work, and in response to public concern, we conducted an audit of the handling of external mail covers. The report was issued in May. For this initial audit, we examined samples of both external criminal mail cover requests and special mail cover files. We are now beginning an audit of internal mail covers.

Federal, State, and local law enforcement agencies can request a criminal mail cover by sending a hard copy form to the Postal Inspection Service's Criminal Investigation Service Center in Chicago. The request must specify the statute thought to have been violated and include a description of how the mail cover will further the investigation. These forms are manually entered into an electronic system for approval. Only the chief postal inspector, the manager of the Criminal Investigation Service Center, or their designees, can approve mail covers.

Most criminal mail covers are approved. In Fiscal Year 2013, the Postal Inspection Service received more than 6,000 outside requests and denied 10.

When a mail cover is approved, it is forwarded to the appropriate facility, where Postal Service staff photocopy the mail pieces or log the information. The facility then mails the records to the Inspection Service to pass on to the original requesters. Requesters are instructed not to copy mail cover records and must return them within 60 days after the mail cover period ends.

Our audit found that mail cover procedures are not always followed.

In 13 percent of cases, external mail cover requests were approved without adequate justification, either because the requester did not include sufficient justification in the request or the justification was not adequately entered into the electronic system;

Authority to approve mail covers was not always delegated appropriately. Twenty-one percent of mail cover requests were not approved by authorized individuals;

The Postal Inspection Service did not ensure that outside law enforcement returned mail cover information on time. In 61 percent of cases, mail cover records were not returned within 60 days as required.

The computer system used to process mail covers had flaws. We found more than 900 cases where the system incorrectly showed a mail cover was active, even though the cover period had ended. System problems also prevented mail covers from being extended and sometimes the same tracking number would be issued to different requests;

There were delays in processing mail covers both by the Postal Inspection Service and at Postal Service facilities.

Finally, the Postal Inspection Service did not carry out its required annual reviews of the program.

Our audit recommended the Postal Service and Inspection Service improve controls over the mail covers program, establish procedures to ensure the required program reviews are conducted, and fix the electronic system. The Postal Service and the Inspection Service agreed with our findings and recommendations and set target dates to implement solutions. Two of the four original target dates have now been extended to March 2015. My office will continue to track the Postal Service's progress.

Mail covers are an important law enforcement tool, but adequate supervision is critical to ensure the protection of the public.

Thank you.

[Prepared Statement of Ms. Whitcomb follows:]

**Hearing before Subcommittee on Federal Workforce,
U.S. Postal Service and the Census
Committee on Oversight and Government Reform
House of Representatives**



Oral Statement

Ensuring Data Security at the Postal Service

November 19, 2014

**Tammy Whitcomb
Deputy Inspector General
United States Postal Service**

Mr. Chairman and members of the committee, thank you for the opportunity to discuss our recent audit report on mail covers. Mail covers have been an investigative tool for more than 100 years, used for tracking financial frauds, drug trafficking, and other criminal activity. A mail cover involves postal officials recording the information from the outside of a mail piece, such as the sender's address. However, the mail cover program does not permit opening letters and packages that are sealed against inspection as this requires a search warrant. To be clear, the program should not be confused with the operational imaging of mail pieces to manage mail flows.

The U.S. Postal Service processed approximately 49,000 mail covers in fiscal year (FY) 2013. Mail covers can be requested either by external investigators, including my office, or by the Postal Inspection Service. There are different types:

- Mail covers that target individuals in suspected criminal matters,
- Mail covers that target postal facilities where mail and parcels associated with criminal activity are passing, and
- Special mail covers used for national security purposes.

The OIG is responsible for auditing the investigative activities of the Postal Inspection Service. As part of this work and in response to public concern, we conducted an audit of the handling of external mail covers. The report was issued in May. For this initial audit, we examined samples of both external criminal mail

cover requests and special mail cover files. We are now beginning an audit of internal mail covers.

Federal, state, and local law enforcement agencies can request a criminal mail cover by sending a hard copy form to the Postal Inspection Service's Criminal Investigations Service Center in Chicago. The request must specify the statute thought to have been violated and include a description of how the mail cover will further the investigation.

These forms are manually entered into an electronic system for approval. Only the chief postal inspector, the manager of the Criminal Investigations Service Center, or their designees can approve mail covers. Most criminal mail covers are approved: in FY 2013 the Postal Inspection Service received more than 6,000 outside requests and denied 10.

When a mail cover is approved, it is forwarded to the appropriate facility where Postal Service staff photocopy the mail pieces or log the information. The facility then mails the records to the Inspection Service to pass on to the original requestors. Requestors are instructed not to copy mail cover records and must return them 60 days after the mail cover period ends.

Our audit found that mail cover procedures are not always followed:

- In 13 percent of cases, external mail cover requests were approved without adequate justification either because the requestor did not include sufficient justification in the request or the justification was not adequately entered into the electronic system.
- Authority to approve mail covers was not always delegated appropriately: 21 percent of mail cover requests were not approved by authorized individuals.
- The Postal Inspection Service did not ensure that outside law enforcement returned mail cover information on time. In 61 percent of cases, mail cover records were not returned within 60 days as required.
- The computer system used to process mail covers had flaws. We found more than 900 cases where the system incorrectly showed a mail cover was active even though the cover period had ended. System problems also prevented mail covers from being extended, and sometimes the same tracking number would be issued to different requests.
- There were delays in processing mail covers both by the Postal Inspection Service and at Postal Service facilities.
- Finally, the Postal Inspection Service did not carry out its required annual reviews of the program.

Our audit recommended that the Postal Service and Inspection Service improve controls over the mail covers program, establish procedures to ensure the

required program reviews are conducted, and fix the electronic system. The Postal Service and the Inspection Service agreed with our findings and recommendations and set target dates to implement solutions. Two of the four original target dates have now been extended to March 2015. My office will continue to track the Postal Service's progress.

Mail covers are an important law enforcement tool, but adequate supervision is critical to ensure the protection of the public.

Mr. FARENTHOLD. Thank you very much.
Mr. EDGAR.

STATEMENT OF TIMOTHY H. EDGAR

Mr. EDGAR. Thank you very much, Mr. Chairman.

I served in the Obama White House as the first privacy and civil liberties official for the National Security Council, focusing on cybersecurity. Under President Bush, I was the deputy for civil liberties for the Director of National Intelligence. And from 2001 to 2006 I was the national security policy counsel for the American Civil Liberties Union.

I am going to talk today a little bit about the history of the privacy of the mail and why that is important.

When I was given this opportunity to testify, many of my friends and colleagues had one Statement: Is nothing sacred? The public is used to a lack of privacy on the Internet. They know about the NSA controversy; they know about Google reading their email for targeted ads. But they expect the Postal Service to have a higher standard for privacy and to be different; and there is a reason for that, which is that, going back to the days of George Washington, the United States has treated mail as something very sacrosanct.

We had a choice in 1792, when the first law was passed establishing the Post Office. We could have gone in a different direction. The European governments of the time had secret rooms in which they monitored mail of political dissidents, of foreign diplomats. The United States decided not to set up such a room and to just ban the opening of mail altogether without a warrant; and shortly after the Civil War, the Supreme Court reinforced that notion, said that a sealed envelope, at least, basically had the same level of privacy as your home, really a pretty remarkable Statement of privacy in correspondence, handled, after all, by a Government agency. So this is an important part of our culture and of our system of constitutional protections for privacy.

During the cold war we got off track. There were several mail monitoring programs run by the CIA and the FBI that were investigated by this Congress, by the Church Committee, in the mid-1970's. The largest of those was called HTLINGUAL. It was a CIA program that actually started as a mail covers program in the early 1950's. The CIA got the cooperation of the Postal Service to obtain copies of every item of mail that was going to or from the Soviet Union, generally in New York.

And it got off the rails in part really just because the CIA did a lot of deceptive tactics to conceal the fact that not only were they photographing the outside of mail, which the Supreme Court had said does not violate the Fourth Amendment, although it should be more highly regulated, but they were actually opening mail as well. They monitored the American Friends Service Committee, they monitored author John Steinbeck. Members of Congress, including Frank Church himself, were on the list of people whose mail should be opened if encountered.

So when this was discovered it was ended, but it had really been a major breach of Americans' privacy and civil liberties. But what are the lessons for today?

I think one important lesson is that the Postal Service needs to be a stickler for privacy. They really need to insist that privacy requirements be followed to the letter, if you will. And they didn't really do that during these cold war abuses. They looked the other way. They allowed other agencies that had important national security missions to trump their concerns. I think they felt this is the CIA, this is national security, let's let them do their thing. And that was the wrong way to go. They needed to be the ones standing up and saying, hey, what are you doing with those pieces of mail? We need to see what you are doing. We need to look and to ask our counsels what is going on.

So that is what is troubling about these missteps by the Post Office, is that you see a certain laxity in the way that they have enforced their rules on mail covers, and that is a troubling one.

Finally, I think this issue of the mail imaging software is an important one for this committee to look at. It may be a separate program from mail covers, but it raises real questions about what is essentially a bulk collection of postal metadata, and it raises questions about the security of those computer files, who has access to them, and privacy risks. Back during the cold war, you actually had to have a program for the CIA to photograph mail. Now that is being done automatically as part of the system delivering it. It may be a separate program, but it raises privacy and security risks, especially with these recent breaches.

Thank you very much.

[Prepared Statement of Mr. Edgar follows:]

Timothy H. Edgar

Watson Institute for International Studies

Brown University

“Data Security at the Postal Service”

Testimony at a hearing before the

United States House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Federal Workforce, U.S. Postal Service and the Census

Wednesday, November 19, 2014

Chairman Farenthold, Representative Lynch and members of the Subcommittee,

Thank you for this opportunity to testify on questions that implicate the privacy of the mail.

I served in the Obama White House as the first privacy and civil liberties official for the National Security Council, focusing on cybersecurity. Under President Bush, I was the deputy for civil liberties for the Director of National Intelligence. From 2001 to 2006, I was the national security counsel for the American Civil Liberties

Union. I am currently a visiting fellow at Brown University's Watson Institute for International Studies, where my work focuses on the policy challenges posed by reconciling security interests with privacy and civil liberties.

"Is Nothing Sacred?"

"Is nothing sacred?" has been the most common reaction of friends and colleagues to the news about privacy problems at the United States Postal Service (USPS). The dismay says a lot about the trust that Americans place in the post office to protect the privacy of their correspondence. We know the NSA collects telephone call detail records, Internet metadata and electronic communications. Major technology companies, such as Google and Facebook, routinely monitor their users to deliver targeted advertising. The post office seemed to offer a last refuge for American privacy. It is indeed alarming that the government is capable of invading our privacy even if we choose to live our lives as complete technophobes, without ever touching a phone or a computer.

The subject of today's hearing is not the opening of mail, which requires a warrant, but the investigative tool known as "mail covers." Mail covers involve copying what appears on the front and back of an item of mail – generally, addresses for a sealed envelope or the contents of postcards or pamphlets. When properly controlled, the tool is an appropriate one for law enforcement and national security investigations, but it carries much the same privacy risks as orders for communications metadata.

Monitoring of mail through mail covers can give the government a revealing picture of a person's life, including who among their friends and relatives is thoughtful enough to send a traditional letter or card, the accounts they maintain at banks and other financial institutions, and the organizations on whose mailing lists they belong. Mail monitoring will also reveal connections with physician's offices, which can reveal very intimate information. The name and address of such correspondence can reveal that a person has a condition that requires a specialist, is seeing a psychotherapist, or has obtained an abortion or family planning services. Physicians often rely on the mail to meet federal privacy requirements precisely because Internet communications are usually unencrypted and therefore insecure.

Unfortunately, the Inspector General of the USPS has found major problems in how the postal service is handling these requests. The USPS authorized 49,000 mail covers in the past fiscal year, a much higher yearly figure than it had previously disclosed in response to Freedom of Information Act requests. The Inspector General's report found that 20% of such mail covers lack the required written authorization. 13% did not include sufficient justification and yet these requests were still granted. The systems for keeping track of mail covers were also faulty. In almost a thousand cases, monitoring continued even after requests had expired.¹

These findings represent more than a few compliance problems at a large federal agency. They shake our confidence in longstanding principles of privacy and civil

liberties that have been a part of the American system since the days of George Washington.

The Privacy of the Mail: Constitutional Origins

The federal constitution gives the Congress the power “To establish Post Offices and post Roads.” In 1792, Congress passed, and George Washington signed, the first permanent law establishing the federal postal service. In that law, Congress flatly prohibited the opening of federal mail. It was a departure from the practices of European governments, who had long maintained secret rooms for monitoring correspondence. In France at the time of the revolution, the room was known as the *cabinet noir* – the “black chamber” – and it was a hated instrument of oppression. The 1792 postal service law would ensure that no such institution would be established in the United States. For more than a century and a half, the privacy of the mail was generally respected, even as newer forms of communication, such as telegraphs, came under broad wartime surveillance, beginning during the presidency of Abraham Lincoln.²

In what appears to be the first case interpreting the Fourth Amendment, the Supreme Court reaffirmed the privacy of the mail. In the 1878 case of *Ex Parte Jackson*, the Supreme Court wrote, “Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in

their own domiciles.”³ The Supreme Court’s message was clear – the right of privacy in personal correspondence was no less important than a citizen’s right to privacy in his home. In both circumstances, a warrant would be required for the government to conduct a search.

Of course, *Ex Parte Jackson* also made clear that this level of protection extended only to sealed correspondence. The “outward form” was exposed to view and therefore not protected by the warrant requirement. The practice of “mail covers” evolved from this distinction. Mail covers allow police and other investigators to track with whom someone is corresponding, without the need to obtain a warrant. It served – and still serves – the same purposes as orders for telephone and Internet metadata today. Indeed, the distinction between the inside and outside of sealed letters and packages provides the basis for the distinction between content and metadata that is crucial to the Fourth Amendment analysis of all forms of communication.⁴

Monitoring the Mail: Cold War Abuses

Between 1940 and 1973, the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) engaged in twelve separate illegal mail monitoring programs. It began with a wartime program to open mail of Axis diplomatic establishments. In 1940, the British taught the FBI what the 1792 law had outlawed: how to secretly open mail. After the war, the government engaged in

much more widespread mail monitoring of ordinary Americans that included both mail covers and illegal mail openings.⁵

The largest of these programs was codenamed HTLINGUAL. It was a CIA program that ran from 1953 to 1973, targeting all correspondence to and from the Soviet Union. This program was run out of New York, where most letters left or arrived. The CIA proposed it as a “mail covers” program and obtained the postal service’s cooperation on that basis. Arthur Summerfield, the Postmaster General, approved the program in 1954, but it appears he never approved opening of mail. In fact, while 215,820 letters were illegally opened, a much larger number – 2.7 million – were photographed, front and back. The monitoring of the outside of mail was therefore more than ten times larger in volume than CIA’s illegal opening of sealed mail. The record is unclear as to whether any subsequent Postmaster General was advised that mail was actually being opened; care seems to have been taken to allow the postal service to be able to deny, at least officially, knowledge of this aspect of the program.⁶

Mail was intercepted first at LaGuardia Airport, then at Idlewild (later Kennedy) Airport by a postal clerk. The clerk received a very sizeable annual bonus of \$500 from the CIA for his cooperation. Mail was delivered to a team of CIA agents in a secret room. They processed 5,000 to 15,000 items of daily correspondence, photographing as many items as possible. A much smaller number – 35 to 75 letters – were surreptitiously selected (“swiped” was the term used by the agents) for later

opening at the CIA's Manhattan Field Office. Each agent who opened mail attended a one-week course called "flaps and seals" at CIA headquarters. The method was simple – the letters were opened using the steam from a kettle and a narrow stick. The CIA attempted to improve the process with a special steam oven capable of handling one hundred letters at a time, but it never worked properly, so agents went back to the tried-and-true steam kettle method.⁷

Agents involved in the program were not foreign intelligence experts and much of the selection was essentially random. Agents were given little guidance on which letters to open, beyond memorizing a "watch list" of persons and organizations of interest, including peace groups such as the American Friends Service Committee, authors including Edward Albee and John Steinbeck, publishing companies, and at least one member of the Rockefeller family. Most of the mail selected was not based on the list. One agent testified that mail was selected "according to individual taste, if you will, your own reading about current events. . . . We would try to get a smattering of everything, maybe the academic field or travel agencies or something." The result of the program was monitoring of Americans for domestic purposes, not foreign intelligence. Over the life of the program, 57,846 items of correspondence were disseminated by the CIA to the FBI.⁸

Despite grand plans for uncovering spies, developing agents inside the Soviet Union, and obtaining valuable foreign intelligence, the record shows that HTLINGUAL's value was doubtful. CIA officials deemed the material "of very little value," describing the

intelligence as “meager.” By the early 1970’s, it had become clear that the program – which officials had always understood was illegal – could create real embarrassment for the CIA and the FBI. It was terminated in 1973, shortly before these and many other Cold War abuses were investigated by a select committee lead by Senator Frank Church.⁹

While the CIA and FBI were directly responsible for the illegal monitoring of mail during these years of Cold War surveillance excesses, the postal service was also to blame. Its officials cooperated with the program. During the initial stages of the program, postal employees were present as the CIA photographed the outside of mail, apparently looking the other way as some letters were “swiped” by the agents. Later, they gave the CIA a separate room where they were left, unmonitored, with sacks of private letters. They knew or at least had strong reason to suspect that the opening of mail was the likely purpose of the program and that it was a crime if done without a warrant. The postal service, and the Postmasters General who knew of the program, did little to raise these legal concerns within successive administrations. The result was monitoring of academics, journalists, innocent travelers and many others – in short, widespread abuse of the rights of Americans.

Lessons for Today

The Inspector General’s report of May 2014 on mail covers does not involve anything on the scale of the illegal mail monitoring uncovered by the Church

Committee, but it is very troubling nonetheless. First, the number of mail covers provided to outside agencies, at 49,000 over the course of the past fiscal year, is well in excess of what had been understood based on the postal service's response to Freedom of Information Act (FOIA) requests. Previous estimates were on the order of 8,000 per year. The discrepancy seems to be the result of the postal service's decision to limit its FOIA responses to law enforcement requests, excluding national security requests and mail covers ordered by its own inspection service. The USPS even attempted to keep this Inspector General report secret.¹⁰ The higher number is troubling in itself. The lack of transparency shown by the postal service is more troubling.

The compliance incident rate found by the Inspector General – 20% of mail covers approved improperly because of a lack of written authorization, and 13% approved without sufficient justification – are likewise not acceptable. By way of contrast, the National Security Agency (NSA), whose compliance missteps have garnered far louder condemnation, has carefully tracked compliance incidents under new Foreign Intelligence Surveillance Act (FISA) authorities. According to a declassified assessment by the Department of Justice and the Office of the Director of National Intelligence, the compliance incident rate – the percent of improperly targeted selectors – for 2013 is less than one half of one percent.¹¹ At least when it comes to compliance, it appears that the USPS has done a far worse job of protecting privacy than the NSA – not what the public might have expected.

As the mail monitoring abuses of the past have demonstrated, vigilance by the postal service is necessary to protecting the rights of the public. The postal service must be a stickler for proper procedure – it cannot afford to be lax, especially when it comes to investigative tools, like mail covers, that require no judicial review or oversight. The USPS should stand for the rights of its customers when it comes to their privacy. Just as customers expect companies like Verizon and Google to insist on proper legal authorization for government data requests, postal customers should expect the same.

The USPS can learn important lessons not only from past abuses involving mail monitoring, but from the actions of the government and industry in responding to recent surveillance controversies. Like the NSA, the USPS can adopt much more rigorous and detailed oversight of its handling of privacy requirements. Like Google and other technology companies, the USPS can publish periodic transparency reports detailing how many mail covers and warrants it processes each year, under what authorities, and how it addresses improper requests. The USPS should fight to make more, not less, information available about national security requests. The DNI is now providing yearly aggregate information about many such requests under national security authorities involving electronic surveillance; there is no reason such information should be withheld when it comes to monitoring the mail.¹²

Finally, the USPS must be careful to avoid the problems created by the NSA's bulk collection of telephone metadata. The system for monitoring the outside of mail

takes advantage of new imaging software that photographs every letter processed by the USPS. This system effectively facilitates a form of bulk collection of postal metadata. While the USPS requires individual suspicion before it approves release of this metadata as part of its mail covers program to requesting state and federal agencies, the existence of the database raises major security and privacy questions.¹³ Congress should scrutinize whether this database is necessary or whether less intrusive alternatives exist, what protections ensure against hacking into the database, how long the data is retained, and who has access to the data. Congress has been debating the NSA's bulk collection of telephone metadata for well over a year. It should ask the same questions of the USPS about this imaging software.

Conclusion

The United States Postal Service is a venerable and trusted institution, with roots going back to the beginning of the republic. History shows, however, that the USPS has not always lived up to the ideals of the nation, or its own ideals, in vigorously protecting the privacy of the mail. These failures were not the result of malice, but of laxity in enforcing privacy requirements. Enforcing these requirements to the letter is the best safeguard against future abuses.

¹ Office of Inspector General, United States Postal Service, "Postal Inspection Mail Covers Program (Audit Report)," May 28, 2014.

² Ralph E. Weber, *Masked Dispatches: Cryptograms and Cryptology in American History, 1775-1900*, at 49-50 (2013); David Kahn, *Back When Spies Played by the Rules* (op-ed), N.Y. Times, Jan. 13, 2006.

³ *Ex Parte Jackson*, 96 U.S. 727, 733 (1878).

⁴ Orin S. Kerr, *Apply the Fourth Amendment to the Internet: A General Approach*, 62 Stanford Law Rev. 1005, 1009-10, 1022-23 (2010).

⁵ Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, Vol. 3, 94th Cong., 2d Sess., Rep. No. 94-755 (April 23, 1976) at 561-67.

⁶ *Id.* at 567-610.

⁷ *Id.*

⁸ *Id.* at 574-75, 632.

⁹ *Id.* at 567-610.

¹⁰ Ron Nixon, *Report Reveals Wider Tracking of Mail in U.S.*, N.Y. Times, Oct. 27, 2014; Josh Gerstein, *Snail mail snooping safeguards not followed*, Politico, June 19, 2014.

¹¹ Semiannual Assessment of Compliance for FISA § 702, June 1, 2012-Nov. 30, 2012 reporting period, at 23 (August 2013), available at <http://icontherecord.tumblr.com/post/58948476651/additional-declassified-documents-relating-to>

¹² Office of the Director of National Intelligence, 2013 Transparency Report (June 26, 2014), available at [http://icontherecord.tumblr.com/transparency/odni transparencyreport cy2013](http://icontherecord.tumblr.com/transparency/odni%20transparencyreport%20cy2013)

¹³ See Nixon, *supra* note 10.

Mr. FARENTHOLD. Thank you very much.
Captain Hamby.

STATEMENT OF CHARLES E. HAMBY II

Mr. HAMBY. Good morning. Thank you, sir. On behalf of Chief Mark Magaw and the Prince George's County Police Department, I would like to thank Chairman Farenthold, Ranking Member Lynch, and the members of the Subcommittee on Federal Workforce, U.S. Postal Service and the Census for the opportunity to discuss the mail cover program and the role this investigative tool plays in our criminal investigations.

My name is Captain Charles Hamby and I am currently assigned as the Assistant Commander of the Narcotic Enforcement Division for the Prince George's County Police Department.

Let me begin by stating that the Prince George's County Police Department is in support of the U.S. Postal Inspection Service mail covers program.

Various investigative units within the police department, including, but certainly not limited to, our fugitive apprehension teams and narcotic enforcement units, have utilized mail covers as supplemental investigative tools to further their cases. Mail covers are able to provide assistance to law enforcement agencies as they are conducting criminal investigations by providing identification information on names and addresses of entities, individuals, and also locations that are associated with the subject being investigated. Fugitive teams may utilize mail covers to identify individuals and locations that could lead to the appreciation of the wanted subject. Narcotic investigations also benefit from mail covers by providing information regarding coconspirators, locations, and methods used by the various activities that occur in drug trafficking.

For example, during an investigation that I conducted of a drug trafficking organization that was smuggling multiple kilograms of cocaine from Miami, Florida to Prince George's County, Maryland, a mail cover was used to develop evidence on one of the 14 co-conspirators. In this case, the mail cover provided identification of names and addresses associated with the target of the investigation, and the specific target was suspected of receiving the proceeds from the drug sales here in Prince George's County and shipping them to Miami, Florida.

The suspect would facilitate the transfer of those funds to the source of supply in Miami, and that money which the suspect was sending to the source was payment for the following shipment of cocaine. During this conspiracy, it was typical for the organization to purchase and receive here in Maryland 10 kilograms or more of cocaine in a single shipment. All of that cocaine was subsequently distributed either in Washington, DC. or in Prince George's County, Maryland.

The information received from that mail cover identified previously unknown aliases that the subject was using. That information led to eventually further identification of the entire system that was being used to pay for the drugs. This case culminated with Federal indictments and successful prosecution of this suspect and her 13 fellow conspirators, which actually resulted in the dismantling of that cocaine trafficking organization.

As described previously, the mail covers used by law enforcement investigators can really provide significant information and further investigations, and also provide evidence of criminal acts.

In closing, thank you very much for the opportunity to present this information to the committee. The mail cover program clearly remains an important tool that continues to benefit criminal investigations by law enforcement agencies. Thank you very much.

[Prepared Statement of Mr. Hamby follows:]



THE PRINCE GEORGE'S COUNTY GOVERNMENT



PREPARED STATEMENT OF

CAPTAIN CHARLES E. HAMBY II
PRINCE GEORGE'S COUNTY POLICE DEPARTMENT

Before the House Subcommittee on Federal Workforce, US Postal Service and the Census
US House of Representatives

Good afternoon. On behalf of Chief Mark Magaw and the Prince George's County Police Department I would like to thank Chairman Farenthold, Ranking Member Lynch, and the Subcommittee on Federal Workforce, US Postal Service and the Census for the opportunity to discuss the mail cover program and the role that this investigative tool plays in criminal investigations conducted by law enforcement agencies.

Let me begin by stating that the Prince George's County Police Department is in support of the U.S. Postal Inspection Service Mail Covers Program. Various investigative units within the police department, including but certainly not limited to fugitive apprehension teams and narcotic enforcement units, have utilized mail covers as a supplemental investigative tool to further their cases. Mail covers are able to provide assistance to law enforcement agencies conducting criminal investigations by identifying names and addresses of entities, individuals and locations that are associated with the subject being investigated. Fugitive teams utilize mail covers to identify individuals and locations that could lead to apprehension of the wanted subject. Narcotic investigations also benefit from mail covers by providing information regarding identification of conspirators, locations and methods used by drug organizations.

For example, during an investigation that I conducted of a drug trafficking organization that was smuggling multiple kilograms of cocaine from Miami, Florida to Prince George's County, Maryland, a mail cover was used to develop evidence on one of the fourteen conspirators. In this case, the mail cover was used to identify the names and addresses associated with a target of the investigation who was suspected of receiving the proceeds from drug sales here in Prince George's County. The suspect would then facilitate the transfer of those funds to the cocaine source of supply in Miami, Florida. This money, which the suspect was sending to the source of supply, was payment for the next shipment of cocaine. During this conspiracy, it was typical for this organization to purchase and receive ten kilograms or more of cocaine in a single shipment.

HEADQUARTERS: 7600 Barlowe Road, Palmer Park, MD 20785

The information received from the mail cover identified a previously unknown alias that the suspect was using. This information led to the full identification of the system used to pay for the drugs. The case culminated with federal indictments and successful prosecution of this suspect and thirteen fellow conspirators which resulted in dismantling this drug trafficking organization. The mail cover was but one of numerous tools used in this case; however, the information gleaned from the mail cover was critical to the success of the investigation.

As described above, mail covers are used by law enforcement investigators when they can provide significant information that can further an investigation or provide evidence of criminal acts. The mail cover remains an important tool that continues to benefit criminal investigations by law enforcement agencies.

Mr. FARENTHOLD. Thank you very much, captain. I have quite a few questions. I do not want to give the mail covers program short shrift, because I think there are a lot of issues we need to discuss with that, but I do want to start with the cyber attacks, since they are most recently in the news. And if I run out of time, we will do a second or even third round of questioning until all the members are satisfied that they have gotten their questions answered.

So, Mr. Miskanic, let me ask a couple questions to reassure the American people. Are we relatively confident that no customer data was compromised during this attack?

Mr. MISKANIC. Chairman Farenthold, as Stated in my written and oral testimony, there was customer call center data that was compromised. It did not contain sensitive information.

Mr. FARENTHOLD. Could you explain what customer call center data is, for those who don't know?

Mr. MISKANIC. Yes, sir. The data itself was when an individual contacts the Postal Service for followup on a mail item or makes an inquiry.

Mr. FARENTHOLD. So you are not going to have their Social Security number or something like that in that data base.

Mr. MISKANIC. No, sir, there was not Social Security numbers contained in that data base.

Mr. FARENTHOLD. All right. What about information or copies of mail cover data or the imaging data that Mr. Cottrell talked about used in the processing of mail, was any of that compromised?

Mr. MISKANIC. No, sir, Chairman Farenthold, there was no indication of compromise of any of the mail cover data, nor of any of the mail imaging data.

Mr. FARENTHOLD. All right. I just wanted to reassure the American folks. Our postal workers obviously appreciate what you all are doing with respect to their credit monitoring.

I am concerned about how long it actually took the Postal Service to act. It was quite some time when CERT notified you all of some data leaking out before you did something. Now, I understand the need to figure out who did it and how it was tracked. Do you see some needs or things that need to be done to, where if the Postal Service is hacked again or another Government agency is hacked, how we can more rapidly shut off the flow of the ex-fill of data and get the tracking tools in the system quicker?

Mr. MISKANIC. Yes, Mr. Chairman. On September 11th, what we were told was there was suspicious activity on four of our pieces of computer equipment, and to give you some scope of that, we have over 225,000 servers or workstations. That indicated that there was simply just suspicious activity or potentially malicious code. Through a complex investigation, we learned that data had actually been compromised.

Mr. FARENTHOLD. Were these mission-critical servers or were they just random servers?

Mr. MISKANIC. These were not our mission-critical servers, they were not our primary and core systems; they were secondary systems. Some of them might have been in a field unit in one of our processing facilities or post offices; some were in our data centers, but they were not necessarily the primary core data centers themselves.

Mr. FARENTHOLD. On my computer network I have software that monitors data flow on my network in my house, and when I see something weird coming out of one of my computers, the first thing I do is go unplug that computer. So, again, would you explain why maybe that wasn't the initial solution and then do forensic investigations to determine where that data was going?

Mr. MISKANIC. Well, in this particular instance, the actor was very sophisticated, and once we had learned the respective access, it was necessary to understand the scope of the intrusion to properly mitigate it. We were very concerned during this period that if the actor themselves could further embed themselves into our network where they could potentially cause harm, it could impact our ability to deliver mail and serve the American public.

Mr. FARENTHOLD. So how much of this was done internally by the Postal Service versus relying on either Government agencies or contractors? I guess what I am getting at, should CERT or the FBI or NSA or some Government agency have a program where you call them and they send in a SWAT team? How was this handled and how do you think it could be handled better?

Mr. MISKANIC. Chairman Farenthold, that is a very good question and, actually, US-CERT does have a SWAT team and the FBI does have a team that came in and assisted the Postal Service with this incident. They provided expert technical guidance. In addition to that, we also relied upon external technical experts from various companies who have been engaged with similar incident response issues.

Mr. FARENTHOLD. Do you think that that interagency system worked well or does it need some polishing? I would certainly say by your time line it needs speeding up.

Mr. MISKANIC. The interagency team was faced with a very complex challenge. It was a very complex investigation in understanding the scope and the breadth across the USPS network and the complexities of that network. We are in the process of still investigating the matter; however, we do intend to produce an after-action report on the actions and activities that occurred during throughout the investigation remediation, and we would be happy to share that.

Mr. FARENTHOLD. I would like to see that. And if there is a classified or security-sensitive version, that would probably be something that this subcommittee probably needs to see in private as well. So please keep us on your list for that.

Sorry, I went a minute over, so we will give Mr. Lynch 6 minutes here.

Mr. LYNCH. All right. Thank you, Mr. Chairman. I appreciate that.

I am going to revisit that in a minute, Mr. Miskanic. Let me ask, though, I only have one question on the covers, the postal covers. Do we have technology that would allow us to read the mail without opening it, read the contents of the mail? I went online to do sort of an anecdotal search about some companies out there that do say we have technology that can read your email without opening it, without indicating to the party who receives the email that their email has been opened and read; and there are a number of firms that actually have very high technology package inspection

that can read through envelopes and see the contents. So I am just wondering if we have the technology available right now to read the mail, the contents of the mail, without opening it.

Mr. COTTRELL. We do not, sir.

Mr. LYNCH. You don't. OK. All right. Who is we?

Mr. COTTRELL. The Postal Service does not have the technology to do that.

Mr. LYNCH. Is it out there?

Mr. COTTRELL. Not that I am aware of.

Mr. LYNCH. OK. It would seem to be pretty simple, just probably high resolution x-ray or something like that. OK, so that is one thing I am concerned about.

As the courts have said repeatedly, there is no expectation of privacy in the outside of what is on your envelope, and that probably makes sense. But my concern is that there may be technology out there that actually would allow folks to scan the outside and also glean whatever the contents of the letter might be as well.

Let's go back to Mr. Miskanic. I really am concerned about the way the Postal Service handled the breach. When were we first aware of this breach of employee data or a breach of the data base at the United States Postal Service?

Mr. MISKANIC. Congressman Lynch, we were notified of the actual data being, we had confirmed the actual data being taken on November 4th.

Mr. LYNCH. No, no, no, no, no, no, no, no, no, no.

Mr. MISKANIC. We had suspected—

Mr. LYNCH. Let's go back. I am talking about when did you first get any indication that you had a breach. I am not talking about official notification.

Mr. MISKANIC. So on October 16th we learned that data had actually been compromised. However, we had fragments of that data and could not—

Mr. LYNCH. OK, so retroactively, looking back, when did you first have a breach?

Mr. MISKANIC. We were notified on September 11th that there was suspicious activity on the system by US-CERT.

Mr. LYNCH. Is that the earliest date that you have right now, have knowledge of, that you had a breach?

Mr. MISKANIC. That I have knowledge of, yes.

Mr. LYNCH. OK. When did you notify the employees that their Social Security numbers had been compromised?

Mr. MISKANIC. We notified the employees on November 10th, and that was due to the need to—

Mr. LYNCH. That is about the day I learned about it, on November 10th, in the Wall Street Journal and New York Times. So why the delay? Why the delay?

Mr. MISKANIC. Over the entire period it was necessary to understand the scope and the impact. Once we learned, on October 16th, that there might have been some data taken, we needed to confirm what that was and reconstruct it forensically. Over that period, it was also very imperative that we initiated remediation and mitigation activity.

Mr. LYNCH. Based on the files, the contents of the files that have been accessed, you should have had some notification right then that there was risk to the employees' data.

Mr. MISKANIC. Sir, during that period, we did not have the full scope of what files were accessed. Second, it was very important for the overall security posture of the Postal Service to conduct the detailed mitigation and remediation that occurred on November 8th and 9th—

Mr. LYNCH. Look, I am just telling you that the way this should work is as soon as you know that a file has been compromised and that it contains personally identifiable information, Social Security numbers, that employee should be notified. If we go with your plan, if we go with your plan, an agency, a U.S. Government agency could have the Social Security numbers for all its employees compromised, and you will decide, you will decide based on your own interests when the employees will be notified that their Social Security numbers have been stolen.

That doesn't work. That doesn't work for the American taxpayer; it doesn't work for the American people. It doesn't. So the secret school squirrel stuff, you know, we have to figure out how sophisticated these people were and what information they have, that doesn't fly. This is very, very important information. These people are at risk and they received zero.

The unions, the employee unions who represent these people got zero notice, like I did, and I am just telling you if we have to do something legislatively to make sure you cough up that information when people's Social Security numbers—you know, I keep hearing about how the private sector has had this problem as well. Target didn't disclose Social Security numbers; Neiman Marcus didn't; JP Morgan didn't. This was all credit card information; this was not their Social Security numbers, which would allow identity theft and an assortment of other problems for these employees.

So I have to tell you I am very, very disappointed in the way you handled this. I am. I think the American people deserve better. And if this is the standard that we are using now, we are opening up a huge area of exposure to the American people. If people like yourself and your agency is going to decide when it is good for you to let people know that their Social Security numbers have been stolen, when you are good and ready, that is not good enough. So we have to figure something out. Maybe it is legislatively we need to mandate this. But you have to be more forthcoming with the people that you are supposed to be protecting than you have been in this case.

I yield back.

Mr. FARENTHOLD. Thank you very much, Mr. Lynch.

We will now go to the vice chair of this subcommittee, the gentleman from Michigan, Mr. Walberg.

Mr. WALBERG. Thank you, Mr. Chairman, and thank you to the witnesses for being here today.

Inspector Cottrell, according to the USPS inspector general, last year only 10 of more than 6700 external law enforcement mail cover requests were rejected. That was given in testimony today. Do you know anything about why those 10 were rejected?

Mr. COTTRELL. I don't know the specifics, sir, but there are specific requirements to get a mail cover: it has to be a law enforcement agency; you have to be investigating the commission of a crime, locating a fugitive or trying to track down victims or assets or proceeds. So those are the requirements, so obviously those 10 did not meet those specific requirements.

Mr. WALBERG. So it would be assumed, then, that it is normal for 99-plus percent of external mail cover requests be approved in any given year?

Mr. COTTRELL. Well, 10 were outright denied. We have to send several back for people to include additional information, but we don't track that sort of data. So 10 were actually denied.

Mr. WALBERG. So we don't know the percentage, normal percentage of a normal year of mail cover requests that are approved in any normal year?

Mr. COTTRELL. It fluctuates year to year. Just this past year we declined 94 of them.

Mr. WALBERG. In your testimony you mentioned the distinction between sealed and unsealed classes of mail. Can you elaborate a little more on that?

Mr. COTTRELL. Well, sealed mail is first class mail sealed against an inspection; you need a Federal search warrant to get inside of that. Other classes of mail are standard, do not have the same level of protection.

Mr. WALBERG. So how does that all impact mail cover?

Mr. COTTRELL. Mail covers are still information from the outside of a mail piece. Standard mail would be advertising mail, circulars, things like that.

Mr. WALBERG. It has been noted that the inspector general audit found that 13 percent of external mail cover requests lacked appropriate justification, yet were still approved. If we were to conduct a full audit of active mail covers today, would the number be any different?

Mr. COTTRELL. I think it would improve. The IG report was from several months ago, and they gave us some excellent recommendations on how to make improvements. What they found is the justification wasn't always included in the system as well. But we have made great strides there and we are continuing to work to improve that process.

Mr. WALBERG. What other recommendations were given?

Mr. COTTRELL. Well, they recommended that we do an annual review of this, which we are doing; they recommended that we improve our mail cover system that we have, where we enter the requesting information in; and they recommended that we train our employees; we fix our internal standard operating procedures. And all of those fixes are in progress.

Mr. WALBERG. The inspector general audit also found that 21 percent of external mail cover requests were approved by individuals without authorization. Has that been changed?

Mr. COTTRELL. Yes, sir. We have made improvements there in improving the delegation process to ensure that we have proper delegations of authority on file for individuals to approve the mail covers.

Mr. WALBERG. So we have them on file, but could you explain a little bit more in depth on how we make sure that, though they are on file, they are actually the ones that are approved?

Mr. COTTRELL. Well, when you delegate authority, you need to have a record that you have delegated that authority, and we did not have proper delegations of authority on file for those individuals, so we have corrected that. We have the correct individuals in place now to approve the mail cover requests that come in.

Mr. WALBERG. Thank you.

Ms. Whitcomb, from your testimony it appears that your audit report focused mainly on mail cover requests made by external law enforcement agencies and that a new report is in the works looking at internal requests. Is that true?

Ms. WHITCOMB. It is true.

Mr. WALBERG. Is there an estimated completion date for that report to end? Are there early conclusions you can share with us today?

Ms. WHITCOMB. Not at this point. We are just beginning that work. But I imagine that we will have some results probably in the next three or 4 months, and we will be happy to come and share those results when we have them together.

Mr. WALBERG. In your testimony you mention that the Inspection Service did not carry out its required annual reviews of the mail cover program. Was your agency able to determine any reason for this failure beyond what we have heard?

Ms. WHITCOMB. Not that I am aware of. They just weren't conducted. I believe one of three of the reviews were conducted. We expected to see annual reviews over 3 years and we saw one review being conducted.

Mr. WALBERG. Are you confident that that is changing now?

Ms. WHITCOMB. Our process is, when we make a recommendation, the agency provides us a response date, a date when the action in response or recommendation is to be completed. In this case the dates that we received in response to our report have been extended, so when those dates or when the Inspection Service has completed their work, they will come back to us and provide us with documentation to show that they have completed that work, and then we will evaluate that and either close that recommendation or can keep it open. So at this point these recommendations are still open, awaiting that documentation to come back to us. So we anticipate that these efforts that are being undertaken will be successful, but at this point it is impossible for us to know.

Mr. WALBERG. Thank you.

Thank you, Mr. Chairman.

Mr. FARENTHOLD. Thank you, Mr. Walberg.

We will now recognize the ranking member of the full committee, Mr. Cummings, for 5 minutes.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. Mr. Chairman, I am extremely concerned about the increased frequency and sophistication of data breaches on both public and private entities. We have seen attacks in the past year at Target, Home Depot, Community Health Systems, and USIS, as well as the Postal Service and, most recently, the State Department.

I am concerned about all Americans whose personally identifiable information was stolen and privacy compromised in a rash of data breaches this past year. That is why I requested four times this year that Chairman Issa join me in conducting oversight into the breaches at these various companies. Unfortunately, Chairman Issa ignored my repeated requests to examine data breaches in the private sector, and this committee has missed a significant opportunity as a result.

Turning to the Postal Service, I must say that I am troubled by the chain of partisanship here. In a joint Statement, Chairman Farenthold and Chairman Issa said they called today's hearing in part because they wanted to know why the Postal Service "waited 2 months before making the news of this attack public." For the record, the Postal Service voluntarily provided to this committee two fulsome and classified briefings, one on October 22d, another on November 7th. Is that right, Mr. Miskanic?

Mr. MISKANIC. Yes, sir, that is correct, October 22d and November 7th, sir.

Mr. CUMMINGS. So we know why the Postal Service did not make this news public earlier, because they told us directly.

Now, Mr. Miskanic has also provided a detailed testimony, including a time line of what the Postal Service knew and when, how and why it made certain decisions, what agencies and experts it has been working with to remediate the breach. That is what I call transparency. By contrast, not a single company that was breached this year came voluntarily to brief this committee.

I am asking Chairman Issa, in his remaining time as chairman, that he finally agree to work with me on ways to improve data security in both public and private entities, and I am hoping that he will agree to my request on January the 14th, September 9th, September 11th, and September 15th.

I would like to thank the Postal Service for working with the committee as it rectifies this intrusion.

Mr. Miskanic, as you know, I wrote to Postmaster General Donahoe last week to request more information on the data breach at the Postal Service. When can I expect a written response?

Mr. MISKANIC. Thank you, Congressman Cummings. We are preparing the written response and we will have it, I believe, within a 2-week period, sir. We are still conducting part of the investigation and would like to provide you a most thorough and detailed response as possible, sir.

Mr. CUMMINGS. And you are saying you will have it in 2 weeks?

Mr. MISKANIC. Yes, sir.

Mr. CUMMINGS. In this year, though.

Mr. MISKANIC. Correct, sir. Yes.

Mr. CUMMINGS. All right.

I am going to ask unanimous consent that letters that I have sent to Chairman Issa requesting investigations into the other entities, private and public, be entered into the record. I have a letter dated September 15th, 2014, September 9th, 2014, September 11, 2014, and January 14, 2014, Mr. Chairman.

Mr. FARENTHOLD. Without objection, so ordered. And I join you in thinking especially the Government needs to do more with re-

spect to data security and look forward to continuing to work with you both this year and in the future.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. I yield back.

Mr. FARENTHOLD. Thank you very much.

We will now to go to Mr. Davis, I guess, for his questions. Oh, Mr. Clay is back. Are you ready, sir?

Mr. CLAY. Yes, I am ready.

Mr. FARENTHOLD. You are up.

Mr. CLAY. I am sorry, Mr. Chairman.

Mr. FARENTHOLD. No, no. We just skipped to Mr. Davis.

Mr. CLAY. OK.

Let me ask Mr. Miskanic. News reports indicated that over 800,000 employees could be affected. We learned that personally identifiable information of Postal Service employees may have been compromised, including names, addresses, dates of birth, Social Security numbers, dates of employment, and other information.

Can you tell us any more information about the extent of people affected by the breach?

Mr. MISKANIC. Yes, Congressman Clay. We are still conducting forensic analysis of the impacted servers and, as a result, as mentioned, we have approximately 800,000 records of current and former employees that had personally identifiable information, the 2.9 million customer care records which were calls to our customer center with either a customer followup. In addition, we are still processing the evidence and there is the possibility of additional compromise specifically as it relates to some workers' compensation files.

Mr. CLAY. Have you identified the perpetrators, or can you discuss that?

Mr. MISKANIC. The adversary we cannot release; it is a classified matter, sir.

Mr. CLAY. Based on your testimony, I understand the Postal Service has been following the advice and guidance of several Federal and private sector cybersecurity experts since the Postal Service's initial discovery of the breach. Is that correct?

Mr. MISKANIC. Yes, Congressman Clay. We have been following the guidance of US-CERT, getting assistance from Carnegie Mellon CERT/CC, and several private security technical experts for this matter.

Mr. CLAY. OK. And I know there has been a great deal of controversy over whether the Postal Service notified its employees and customers about the breach in a timely manner, but it seems to me that the Postal Service relied heavily on the intelligence and expertise it was receiving from its advisors in making these determinations.

For example, in your testimony you stated that experts from supporting agencies provided prudent warnings that short-term remediation efforts would be seriously compromised if the threat actor became aware that the intrusion had been discovered. If provided advance warnings of network actions intended to expel and block the intruder from the Postal Service network, the advisory could take bolder steps to further infiltrate or sabotage systems.

Mr. Miskanic, is this why the Postal Service chose not to inform its employees and customers about the breach when it was originally discovered in mid-September?

Mr. MISKANIC. Yes, Congressman Clay. The concern that was raised by the technical experts both from the Federal Government and the private sector regarding the adversary potentially conducting malicious acts were very significant and could have harmful impacts for our ability to deliver the mail to each and every American citizen, and we wanted to ensure, first of all, protect any further breach of data, but ensure that those systems were adequately protected and then implement the mitigation activities, which are quite complex. We are in the first phase of several phases for those mitigation activities, and they will go on for several months.

Mr. CLAY. And I understand that the Postal Service agreed to offer free credit monitoring for its employees for 1 year, is that correct?

Mr. MISKANIC. That is correct, sir, free credit monitoring and identity theft protection, sir.

Mr. CLAY. And based on your experience in handling these issues, are you confident that the Postal Service will be able to effectively address the current data breach and prevent further breaches from occurring in the future?

Mr. MISKANIC. Yes, sir, I am confident, and you have our commitment that we will address all of the issues and be very vigilant in the future, sir.

Mr. CLAY. And you cannot tell us if you have identified the culprit.

Mr. MISKANIC. No, sir. I believe that is a matter that is best discussed with the intelligence community, sir.

Mr. CLAY. I see. Thank you for your responses.

I yield back, Mr. Chairman.

Mr. FARENTHOLD. Thank you very much.

Mr. Davis?

Mr. DAVIS. Thank you very much, Mr. Chairman. I want to thank you and the ranking member for giving me the opportunity to participate in this hearing, though I am not a member of this subcommittee.

Like several of my colleagues, I am concerned about the length of time that it took to notify employees, as well as customers, of the breach. Mr. Miskanic, can you share something by November 10th that you had learned that you didn't know, say, September the 11th that gave you the level of comfortability to now notify these individuals of the breach that had not been notified earlier?

Mr. MISKANIC. Sir, on September 11th we had no indication that there was data that was compromised or accessed in an unauthorized manner; we simply had information that there were four servers out of several hundred thousand workstations that had potentially malicious code on them. In order to adequately investigate, over the period of the next 2 months, we had to come to learn the sophistication of the actor and then came to find that they had indeed compromised data; however, we had fragments of that data and needed to recreate that to make the adequate notice to our employees.

On November 4th is when we actually confirmed through our investigation that that information had indeed left the Postal Service network, and not before that time, sir.

Mr. DAVIS. So the investigation then gave you the information that you needed to have in order to have a level of assurance that what you were announcing or reporting was in fact accurate and adequate. Let me ask you have there been any interactions or conversations with representatives of the employees, such as the unions, to discuss the issue and see how jointly the Service and the employees may be able to work together finding a solution?

Mr. MISKANIC. Individually, I have not engaged with those discussions; however, I know the postmaster general and staff have engaged the unions, and they will continue to engage them throughout this entire process.

Mr. DAVIS. Thank you very much.

Let me ask you, Captain Hamby. I understand that you have been involved in this kind of activity for a pretty extensive period of time. How valuable do you view the mail covers program?

Mr. HAMBY. Congressman Davis, I think it is a very valuable tool. It is not used that often, quite frankly, in investigations, it is only when it is warranted; and usually it takes time, it is usually in a long-term investigation that is going to be used in any event.

But in my experience, it provides a very unique piece of information in criminal investigations. There are so many types of information out there. The mail cover can provide very, very unique pieces of information, so in that instance it is very valuable. It really can't be duplicated as far as mail coming and going from a specific address.

Mr. DAVIS. Thank you very much.

Mr. Miskanic, let me just reinforce that the employees that I have been speaking with or have had conversation with, I guess they, like others, are very skeptical when they think that there has been some breach of their information. So I think they would be reassured to know that the Postal Service is in fact interacting with their leadership to try and find a resolve, so I thank you very much.

And I thank all of you for your participation and the questions that you have answered.

Mr. Chairman, I yield back.

Mr. FARENTHOLD. Thank you very much.

I think we have gotten to everybody, so we will startup with a second round of questioning and I will kick it off.

Mr. Miskanic, you will be happy to know you have almost all my questions answered. I want to go on to the mail covers program a little bit more.

Mr. Cottrell, the IG's report has a picture of a guy writing down information off of a package, and your testimony said often this is done manually. How much of this is done electronically? Is it just photocopied, is it scanned? Can you break down the percentages of how that data is captured?

Mr. COTTRELL. Yes, Mr. Chairman. It is all done manually. The only electronic piece would be to actually photocopy the pieces of mail. That is the only electronic part of this process. It is all manual.

Mr. FARENTHOLD. And you also mentioned that you have some internal programs where you actually image the covers of the mail for processing.

Mr. COTTRELL. Yes, sir.

Mr. FARENTHOLD. So that is basically where you scan the front, bar code the address. How long is that stored, and are those computers on a network that do that?

Mr. COTTRELL. Those mail processing machines are at all of our facilities around the Country. The images are only on that one mail processing machine and the data is overwritten depending on the volume of the mail processing machine.

Mr. FARENTHOLD. So are we talking days, weeks?

Mr. COTTRELL. Days. Three to 7 days.

Mr. FARENTHOLD. All right. Can you assure me that there is not some NSA-like system that is tracking all mail covers, storing that data for later search and retrieval?

Mr. COTTRELL. Yes, I can. There is no such system in the Postal Service doing anything like that.

Mr. FARENTHOLD. And can you tell me is there a similar process for mail covers for shipments made through your competitors, UPS, FedEx, and the like? Are you aware of any similar programs?

Mr. COTTRELL. I am not aware of any.

Mr. FARENTHOLD. Mr. Edgar, you are the privacy expert. How is the Postal Service different from FedEx and UPS?

Mr. EDGAR. I don't believe there is any real difference here, but the point I was trying to make, I think, in my written Statement about this concern is just that the data is potentially vulnerable. We have heard about data breaches of other systems at the Post Office, so it is important to really look very closely at how this data is stored and how it—

Mr. FARENTHOLD. As a Government efficiency expert, it troubles me that there has to be a hard copy request that is then entered into a data base that is then sent to the local post office and is then done manually, and then I guess you mail the mail covers to the law enforcement agent. So, as a government efficiency expert, that troubles me. As a privacy advocate, I kind of like it.

Mr. EDGAR. I think that is a good point. I think that in some ways my personal fears about this were probably in part because I didn't realize how inefficient the mail covers program was. And maybe that is a good thing because it allows us to, as we improve the mail covers program and if there is any effort to integrate it with any of these systems, to do it in a very careful fashion.

Mr. FARENTHOLD. Right.

Let me go on. Mr. Cottrell, what about the contents? Are there drug dogs that check? There has to be some additional stuff for the contents so you guys aren't at least doing something to combat the belief that you are the biggest deliverer or contraband in the world.

Mr. COTTRELL. Absolutely not. The U.S. mail should not be the provider of choice for narcotics. That is why you see this spike in mail covers is indicative of our efforts to combat this very offense. But to raise the level, to get into a package, obviously you need to get to probable cause. Sometimes that is one method, but a hit with a drug dog is obviously one of the ways we can get that problem.

Mr. FARENTHOLD. Ms. Whitcomb, you talked about the designees. Do you know how many designees there are that authorize mail covers and what kind of training that they receive?

Ms. WHITCOMB. I don't know the answer to that question.

Mr. FARENTHOLD. Mr. Cottrell, do you know?

Mr. COTTRELL. I am sorry, Mr. Chairman, could you repeat that?

Mr. FARENTHOLD. How many designees are there to authorize mail coverings and what kind of training do they receive.

Mr. COTTRELL. I would like to give you a full and thorough answer. I believe there are two, but if I could provide an answer for the record.

Mr. FARENTHOLD. And then we talked about how few of the requests were denied. Were they denied on substantive grounds or were they denied because all the Is weren't dotted and Ts crossed? Mr. Cottrell or Ms. Whitcomb, either one.

Mr. COTTRELL. It would be because they did not meet those requirements of it is from a law enforcement agency, it is looking to obtain evidence in the commission of a crime, locate a fugitive.

Mr. FARENTHOLD. So you all really don't have that many substantive checks, it is predominantly that you have met all the requirements; it is not like a judge reviewing a search warrant or something like that.

Mr. COTTRELL. It is not, but it has to be a sworn law enforcement agency.

Mr. FARENTHOLD. OK. Finally, I want to ask one question about you said the policy was 60 days to you send the mail covers to a law enforcement agency, they have 60 days to return them. I guess Ms. Whitcomb said that. How does that work? It seems to me that if my mail covers were used in a prosecution, I would want to have access to those mail covers and there needed to be preserved through the process of—I would want my defense attorney to have access to those if I were prosecuted as a result of those. Anybody want to comment on how that is mailed available to the defendants in a criminal proceeding? Either of you guys know?

Mr. COTTRELL. They could request an extension to retain that for a trial purpose.

Mr. FARENTHOLD. OK. That just kind of struck me as being an issue. Thank you very much.

Mr. Lynch, you had some second questions?

Mr. LYNCH. Please, yes. Thank you, Mr. Chairman.

Mr. Miskanic, I want to go back to the 800,000 postal employees who had their Social Security numbers stolen. In that file that had their names, addresses, and Social Security numbers that were stolen, that information would be very helpful to someone engaged in identity theft, would it not?

Mr. MISKANIC. Yes, sir, that information could be used for identity theft.

Mr. LYNCH. So I am just wondering do we have, part of the thing I am struggling with is that it took so long for us to figure out, for the Postal Service to figure out what the adversary stole. And you would think that the Social Security numbers, names, and addresses of our 800,000 employees would be sensitive information that might be segregated so that it might gain greater protection. You follow me?

Mr. MISKANIC. Yes, sir.

Mr. LYNCH. So I know we encrypt it, but we encrypt it. We should be able to know what has been stolen. Just a basic concept there. How come it took so long for us to figure out that they had stolen the Social Security numbers, addresses, and names of 800,000 postal employees? I can't understand that piece. Can you explain it?

Mr. MISKANIC. Yes, sir. The adversary had encrypted the file that had been taken themselves and produced a new name of that file, and we had to decrypt that file to understand that that had actually been stolen and left the USPS network.

Mr. LYNCH. But if we had segregated that file and knew it had been accessed, as was reported on September 11th, then we could have alerted people that we are concerned. The thing for me is if someone has my Social Security number, the best defense is for me to know that so that, as a consumer, I can watch out for my savings account, credit card activity, things like that. But if I don't have that information, I am defenseless.

So that is what I am getting at. If we knew that that file had been accessed, like we knew on September 11th, it just raised a red flag to the people who might be vulnerable because of that intrusion. That is what I am trying to get at.

Mr. MISKANIC. Sir, we did not know that that file was accessed on September 11th. On October 16th we had partial information that there was fragments of a file that were recovered that had been deleted by the adversary. Through that period of time we needed to adequately reconstruct what happened to make notice to our employees, because we didn't know if it was one or 800,000 at the time.

Mr. LYNCH. But we knew that there were four servers that were accessed on September 11th, is that correct?

Mr. MISKANIC. Which none of them contained this information; it was a different vector of the attack, sir.

Mr. LYNCH. Well, we need to figure out a way that the most sensitive information that we have on these employees that would introduce severe vulnerability on behalf of our employees, we need to find a way to segregate that so if it is accessed or if there are indications it has been tampered with, that we can notify them. Are we doing that now as part of this corrective action or can we expect this to happen again?

Mr. MISKANIC. Sir, we have actually segregated systems for our most critical data. Unfortunately, this was a sub-business process, a reporting process that caused this file to be subject to a vulnerability. We have corrected that issue. We will continue to correct any of those issues in moving forward to ensure that this doesn't occur again.

Mr. LYNCH. OK. I am concerned about this because so far what I see is there is no negative consequences to the United States Postal Service because these 800,000 employees' Social Security numbers were stolen. Zero. Nothing bad is going to happen. And we are lining up here that it is business as usual and, oh, this happened in the private sector. The private sector, customers will move away from a company that is not protective of their information.

We have a captive audience in the employees of the American Postal Workers Union and some of the other workers there as well, so I am just concerned about a perverse incentive here that if there is no negative consequences to what just happened, it is going to happen again. I am just trying to avoid that eventuality and I am having trouble getting cooperation to make sure that doesn't happen. I think we are whistling through the graveyard here and we are not taking it seriously enough.

Tell me I am wrong.

Mr. MISKANIC. Sir, you have our full cooperation and commitment that we will continue the efforts that we have undertaken to remediate the impacts of this breach and continue to improve our systems and our networks. This is a very sophisticated adversary and it is necessary for the Postal Service then to learn the traits of the sophisticated adversaries. We look forward to working with our Federal Government partners to better learn those tactics. I can assure you that we will improve our systems in the future.

Mr. LYNCH. Thank you, Mr. Miskanic.

I yield back.

Mr. FARENTHOLD. Thank you very much.

Mr. Cummings, you have some more questions for us?

Mr. CUMMINGS. Yes, I do. Yes, I do.

Let me ask you this. Tell me what is the likelihood of this happening again? I know you are still looking into it. I always talk about transformational moments that should lead to a movement. Sometimes when these kinds of things happen, it makes us realize how vulnerable we are, and we constantly say to ourselves that when the rubber meets the road, that we will be prepared; and then when it comes time for the rubber to meet the road, we discover there is no road. So I am just trying to figure out what the likelihood of this happening again is and exactly what are we doing to make sure it doesn't, if we can.

Mr. MISKANIC. As you Stated, Congressman Cummings, this is a transformational moment in the way that the Postal Service addresses IT security. It is necessary for us to be more actively engaged with these emerging threats that are well resourced and have a long time period to affect their activities. No IT security professional can State unequivocally, 100 percent, that they will never be breached again, but we must remain vigilant and we must improve our processes to ensure that it does not.

Mr. CUMMINGS. Do we have the necessary people with the appropriate skills and technology to address these problems or is more needed?

Mr. MISKANIC. Speaking from the Postal Service, that is what I have been tasked with, is understanding if we have the proper skills and technology.

Mr. CUMMINGS. You are saying you are trying to figure that out, is that what you are saying?

Mr. MISKANIC. We are embarking upon that because obviously, sir, we need to improve our skills and our tools and our tactics to ensure this doesn't happen again.

Mr. CUMMINGS. And what will it take to do that? In other words, are there people out there that we are not benefited or worked with to get their expertise? Do we have it in-house? Do we need to go

out-house? I mean, what is needed? Because I have some of the same concerns as Mr. Lynch and others. It is one thing for things to go wrong, and we realize that you said, there is no 100 percent failsafe system. We got that.

But I want to know that we are doing, and I think the American people want to know that we are doing the very best that we can. So if there is a lack of anything, we want to know exactly what it is and what we can do about it.

Mr. MISKANIC. To adequately fight these very significant and persistent threats, it is necessary that we form teams that are both across the Federal Government and the private sector. In the case of Postal Services is ensuring that we are actively engaged with obtaining the information on the threat actors from the intelligence community to process that and make it actionable and put it into tactics to better protect the USPS network.

Mr. CUMMINGS. One of the purposes of this hearing is to evaluate the Postal Service's progress in implementing the recommendations made by the Postal Service Office of Inspector General. Ms. Whitcomb, your office made four recommendations to the Bureau as it relates to mail covers program, is that correct?

Ms. WHITCOMB. Yes.

Mr. CUMMINGS. And Chief Inspector Cottrell, does the Postal Service agree with all four of those recommendations?

Mr. COTTRELL. Yes, Ranking Member Cummings.

Mr. CUMMINGS. But based on your testimony, I understand that you have completely implemented one of the recommendations, is that correct?

Mr. COTTRELL. That is correct.

Mr. CUMMINGS. I would like to discuss this recommendation in detail. First, based on your testimony, I understand that the Inspection Service has already implemented periodic review procedures that the IG recommended, is that correct?

Mr. COTTRELL. Yes, that is correct.

Mr. CUMMINGS. And, chief inspector, can you tell us a little bit more about the revisions you made to review the procedures that you discussed in your testimony?

Mr. COTTRELL. Yes. Just briefly, Congressman, every year we go out and we review our high risk programs, and we have added this mail cover review to our annual review of high risk programs, and we have already begun those reviews in response to the IG's recommendations.

Mr. CUMMINGS. And so the other recommendations, what about those?

Mr. COTTRELL. Those are still in progress. Some of them involve IT upgrades and issues, and the training and getting folks trained, and republishing our standard operating procedures and some of our internal training manuals. But we do expect to be complete in the timeframe the IG allotted.

Mr. CUMMINGS. Do you think you have the resources to accomplish all of that?

Mr. COTTRELL. Yes, I do.

Mr. CUMMINGS. All right.

Thank you very much, Mr. Chairman.

Mr. FARENTHOLD. Thank you very much.

Mr. Davis, do you have some more questions?

Mr. DAVIS. Yes, Mr. Chairman. Thank you very much.

I would just like to followup a little bit more on the recommendations that have been made and how effective we think we have been in completing those or in coming up with the processes used to complete those recommendations.

Mr. Cottrell, could you embellish that a bit?

Mr. COTTRELL. Yes, Congressman. What the IG found is that opportunities exist to improve our controls, so there are several controls in place, so they recommended we establish improvements to ensure responsible personnel process mail covers as required; establish procedures to ensure that periodic reviews, as we spoke about; ensure mail covers are processed in a timely manner; and implement controls to ensure data integrity.

Likewise, we are reviewing and updating our standard operating procedures, our instructions to our own employees, as well as to outside law enforcement agencies, and we are updating our internal training guides as well, to be sure. We are also developing a disbarment process for external agencies for noncompliance, so that we can bar them from ever getting mail covers again. So we have uncovered some additional things we would like to do, in addition to what the IG recommended as part of that review to make it a stronger, tighter process.

Mr. DAVIS. Ms. Whitcomb, would you agree with this assessment?

Ms. WHITCOMB. The actions that they have undertaken sound very responsive to the recommendations that we have made, but I have to say that we haven't made an assessment of the actions that they have taken in response to our recommendations. As I mentioned, we are looking into internal mail covers now and, as a part of that, will likely check in on the actions that they have taken in response to our recommendations on the external mail covers.

Mr. DAVIS. Well, thank you very much. It appears to me that we are indeed making progress.

Mr. Chairman, I have no further questions and yield back the balance of my time.

Mr. FARENTHOLD. Thank you very much.

I just have two quick questions. Mr. Lynch says he has another question, so we will do a quick third round of questions.

Captain Hamby, Mr. Cottrell and Ms. Whitcomb basically indicated that if a law enforcement agency dots all the Is, crosses all the Ts, it seems like it is almost certain that they will get approval of the request for covers. Can you talk a little bit about how you found out about this program, how you were trained about it, how you train your personnel in how to use it, and a little bit about the decisionmaking process to make sure it isn't abused to infringe upon the privacy of an individual person, yet still available to track the bad guys?

Mr. HAMBY. Yes, sir, Chairman Farenthold. As far as learning about the program, as investigators, our investigators start out with basic training in the police department. We are talking about my agency here. To become an investigator, you pretty much have to prove your metal; you get selected as an investigator, then you go to basic investigator school. It will be mentioned in basic investi-

gator school, but for narcotic investigators this is one of the tools that you would learn about in narcotic investigator school.

As far as utilizing it as an investigator, as the new investigator, you are usually paired with one who has more experience, and this is one of the tools, like many of them, that this isn't a fishing expedition tool; this is an initial tool. This is one that is only used, in my experience—and I have been doing this as a narcotic investigator for 12 years—we have only used this tool when there are reasonable grounds.

Mr. FARENTHOLD. Is there management approval for it or can any investigator just request? Suppose some investigator wants to make sure her spouse isn't sending love letters to somebody else.

Mr. HAMBY. Yes, sir, there is, and the process is, first of all, the completion of the request form for the U.S. Postal Service, but it also requires a cover letter from a supervisor; and that supervisor would have to complete the cover letter and notify his commander. So that is the process we would use in our agency to ensure that requests are authorized throughout our agency, and it would be in the Postal Service.

Mr. FARENTHOLD. Thank you very much.

Mr. Miskanic, your answer to another question suggested another question for me. I am sorry, you are not off the hook from me yet. You indicated that there were four servers that were breached, but this sensitive data did not reside on one of those four servers. So I am assuming those four servers were used as a gateway to further penetrate the network. Can you tell us how many devices or servers were penetrated?

Mr. MISKANIC. Yes, Chairman Farenthold. Approximately 100 servers were penetrated. And to give you some scope, there is approximately larger servers like that. It is over 25,000, and then there are, like I mentioned, over 200,000 workstations. So 100 workstations and/or servers were impacted.

Mr. FARENTHOLD. Was there any indication, and if I am getting into a classified area, please stop me and we can talk about this in an appropriate environment for that. Was there any indication that there was more sensitive information other than employee data that was targeted?

Mr. MISKANIC. There is no indication o that at this present time, sir.

Mr. FARENTHOLD. OK. Thank you very much.

Mr. Lynch?

Mr. LYNCH. Thank you.

Mr. Miskanic, the Social Security numbers for the 800,000 employees, I understand in one of these reports say those were copied by the adversary. Is that correct?

Mr. MISKANIC. Yes.

Mr. LYNCH. So we don't have to worry about them coming back and trying to hack that portion of it, because they have that information.

Mr. MISKANIC. They copied a file, sir, yes.

Mr. LYNCH. Yes. So how are we helping out these employees because their information is out there now?

Mr. MISKANIC. We are providing, through a commercial service, creditor monitoring to them and also identity theft protection. In

addition to that, through our human resources service center, we have contact numbers for them to contact us if they need additional details or if they suffer any negative consequences.

Mr. LYNCH. OK. I am pretty sure, I have a bunch of family that work for the Post Office and I am sure they have employee numbers. Is there any thought to creating a firewall by discontinuing the use of Social Security numbers, which the vulnerability is far greater than would be if we were using an employee number to identify these folks?

Mr. MISKANIC. As part of our undertaking, we look at all of our data retention policies, data storage policies, which includes the storage of personally identifiable information. That is an excellent suggestion, sir, that we have undertaken previously, but obviously we need to also consider the further use of that. There are in some instances the need, from a payroll reporting perspective, to have a Social Security number, but it is, first and foremost, something that we are doing to see if we can shield those in some other way possible to make them less vulnerable or not vulnerable at all for theft.

Mr. LYNCH. OK. And the wider group, including the folks that complained, they called the customer call office, their information was compromised as well. How many of those were there?

Mr. MISKANIC. There was 2.9 million records that were taken.

Mr. LYNCH. That is on top of the 800,000 employees?

Mr. MISKANIC. That is correct, sir. That did not contain any sensitive information; it was essentially their name and address, and if they left a telephone number.

Mr. LYNCH. Are we looking at how long we hang on to that information?

Mr. MISKANIC. That is something we are doing as well. The data retention policy for the entire Postal Service will be under review, and specifically how long we hold that customer data is very first and foremost that we need to understand whether we have a business need for that or not, sir.

Mr. LYNCH. OK. Thank you, Mr. Miskanic.
I yield back.

Mr. FARENTHOLD. Thank you very much.

Mr. Cummings, you have any more?

Well, thank you all very much. I really do appreciate the panel taking their time to answer our questions. We have a couple of followups we look forward to hearing from you on. We appreciate your service to the Country and/or your communities.

With that, we are adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL B. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. LEAHY, NORTH CAROLINA
JIM COHRAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMode, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT D. HARTZ, TENNESSEE
TROY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DICK HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WYCHALL, GEORGIA
THOMAS MACISE, KENTUCKY
DANIEL J. RYAN, CALIFORNIA
MARK BEADLOW, NORTH CAROLINA
KERRY L. BENNETT, MICHIGAN
RON D. SANTIS, FLORIDA

LAURENCE J. GRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

Majority (201) 225-5874
Fax: (202) 225-5874
Minority (202) 225-4251
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MEMBER

CAROLYN B. MALONEY, NEW YORK
CLEANER HODGES, DISTRICT OF COLUMBIA
JOHN F. THUNE, MASSACHUSETTS
JON LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACOB SPIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
MARK RUCAN, MISSOURI
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY GRIFFIN, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
ANGELLE L. GRIFFIN, NEW MEXICO

January 14, 2014

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Since last October, the Committee's top priority has been investigating the security of the Healthcare.gov website and the risks posed by domestic hackers, foreign entities, and others seeking to harm our national interests. This investigation has involved numerous public hearings, tens of thousands of documents obtained from federal agencies and private contractors, and multiple transcribed interviews. Thankfully, to date there have been no successful security attacks against the Healthcare.gov website, although the increasing frequency and sophistication of attacks against all federal information technology systems increases the risks of such a breach.

Unfortunately, while the Committee was conducting its investigation during this time period last fall, up to 110 million Americans were subjected to one of the most massive information technology breaches in history when their credit, debit, and other personal information reportedly was compromised at Target stores and online in November and December.¹

I am writing to request that the Committee hold a bipartisan hearing with senior Target officials and security experts to investigate the cause of this breach, its implications for American consumers, and the steps Target has taken to address this specific breach and implement mitigation measures to ensure that similar attacks are not successful in the future. In addition to serving the interests of millions of American consumers affected by this breach, I believe the Committee could learn from these witnesses about their failures, successes, and best practices in order to better secure our federal information technology systems.

According to security experts, "the kind of information stolen—including names, card numbers, expiration dates and three-digit security codes—could allow criminals to make

¹ *For Target, the Breach Numbers Grow*, New York Times (Jan. 10, 2014) (online at www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0).

The Honorable Darrell E. Issa
Page 2

fraudulent purchases almost anywhere in the world.”² Millions of these stolen credit and debit accounts reportedly “have been flooding underground black markets in recent weeks.”³ Based on recent news accounts, it is unclear why Target had inadequate security measures in place,⁴ why the breach was not detected sooner,⁵ and whether the full extent of the breach has been uncovered.⁶

One of the most significant questions is why Target did not notify customers sooner.⁷ Although initial accounts in December reported that approximately 40 million consumers had been affected,⁸ it was reported in January that more than 100 million consumers may have been affected.⁹

You and other House Members have cited the Target breach to justify legislation relating to the Healthcare.gov website. Last Friday, during floor debate on H.R. 3811, The Health Exchange Security and Transparency Act, the bill’s sponsor, Rep. Joseph Pitts, began debate on the bill by stating:

Mr. Speaker, in the days leading up to Christmas, hackers stole millions of credit card numbers from the servers of retail giant, Target. I imagine that at least a few here in this chamber may have had their own credit cards replaced to prevent theft. What if Target had not bothered to tell anyone? What if they had waited until people noticed

² *Target Says 40 Million Credit, Debit Cards May Have Been Compromised in Security Breach*, Washington Post (Dec. 19, 2013) (online at www.washingtonpost.com/business/technology/target-data-breach-affects-40-million-accounts-payment-info-compromised/2013/12/19/5cc71f22-68b1-11e3-ae56-22de072140a2_story.html).

³ *Target Data Breach Spurs Lawsuits, Investigations*, USA Today (Dec. 23, 2013) (online at www.usatoday.com/story/money/business/2013/12/22/target-breach-suits-and-investigations/4167977).

⁴ *Id.*

⁵ *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, Reuters (Dec. 19, 2013) (online at www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219).

⁶ *Target Says Data Breach is Far Larger Than First Estimated*, Los Angeles Times (Jan. 10, 2014) (online at www.latimes.com/business/la-fi-target-breach-20140111,0,987578.story#axzz2qKAGeErR).

⁷ *Why Did Target Take So Long to Report Data Security Breach?*, CNBC (Dec. 20, 2013) (online at www.nbcnews.com/business/why-did-target-take-so-long-report-data-security-breach-2D11783300).

⁸ *Target Says 40 Million Credit, Debit Cards May Have Been Compromised in Security Breach*, Washington Post (Dec. 19, 2013).

⁹ *For Target, the Breach Numbers Grow*, New York Times (Jan. 10, 2014) (online at www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html).

The Honorable Darrell E. Issa
Page 3

fraudulent charges popping up on their statements? The damage would certainly be worse.

Later in the debate, you invoked the Target breach, stating: "no private sector company, including Target, would go live with a system that has known failures and unknown failures because of a failure to do end-to-end."

During a television interview yesterday, Target's Chief Executive Officer, Gregg Steinhafel, explained his company's approach to handling this crisis:

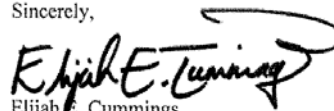
As time goes on, we are going to get down to the bottom of this. We are not going to rest until we understand what happened and how that happened. Clearly, we are accountable, and we are responsible. But we are going to come out at the end of this a better company. And we're going to make significant changes. I mean, that's what you do when you go through a period like this. You have to learn from it, and you have to apply those learnings. And we're committed to do that.¹⁰

I believe this is a positive overall approach, but it will take oversight to ensure that the company follows through on its responsibilities. As Majority Whip Kevin McCarthy stated in the context of the Healthcare.gov website: "Nothing can turn a life upside down more quickly than identity theft. It is our duty to do everything we can to inform Americans."¹¹

For these reasons, I request that the Committee engage with Target, in a collaborative and bipartisan way, not only to help protect the millions of consumers affected by this massive breach, but to learn lessons that can help us improve federal information technology systems and procedures.

Thank you for your consideration of this request.

Sincerely,



Elijah E. Cummings
Ranking Member

¹⁰ *Squawk Box*, CNBC (Jan. 13, 2014) (online at <http://video.cnbc.com/gallery/?video=3000235005>).

¹¹ *House Passes Obamacare Security Measure*, Politico (Jan. 10, 2014) (online at www.politico.com/story/2014/01/house-passes-obamacare-security-measure-102018.html).

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MCHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LAMARCA, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK RHEENAN, PENNSYLVANIA
SCOTT DUKAKIS, TENNESSEE
TROY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DIP HOS THINS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DAVID CDLOND, GEORGIA
ANDREW MCDONNELL, NORTH CAROLINA
KERRY L. BENNY, MICHIGAN
RON DESANTIS, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

RECAPITULATED (202) 225-5874
FACSIMILE (202) 225-5874
TELEPHONE (202) 225-5851
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

September 9, 2014

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am writing to request that the Committee hold a bipartisan hearing to investigate the causes and effects of a very serious data security breach at Community Health Systems, Inc., the nation's largest for-profit hospital chain.

Last month, Community Health Systems, which operates 206 hospitals across the United States, announced that hackers broke into its computers and stole data on 4.5 million patients.¹ This represents the second largest health information breach in history and the largest hacking-related health information breach ever reported.² Hackers reportedly operating from China gained access to patient names, Social Security numbers, physical addresses, birthdays, and telephone numbers, putting these individuals "at heightened risk of identity fraud."³

Over the past year, the Committee has been investigating the security of the Healthcare.gov website. This investigation has involved numerous public hearings, more than a million pages of documents from federal agencies and private contractors, and 18 transcribed interviews. To date, however, no personally identifiable information has been compromised as a result of malicious cyber attacks, although outside actors have repeatedly tried.⁴

¹ *Hack of Community Health Systems Affects 4.5 Million Patients*, New York Times (Aug. 18, 2014) (online at <http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients>).

² *Hackers Directly Targeting Health Care Organizations, FBI Warns*, iHealthBeat (Aug. 21, 2014) (online at www.ihealthbeat.org/articles/2014/8/21/hackers-directly-targeting-health-care-organizations-fbi-warns).

³ *Hospital Network Hacked, 4.5 Million Records Stolen*, CNN Money (Aug. 18, 2014) (online at <http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack>).

⁴ See, e.g., *HealthCare.gov Server Hacked. But HHS Says No Consumer Information Taken*, Washington Post (Sept. 4, 2014) (online at www.washingtonpost.com/blogs/the).

The Honorable Darrell E. Issa
Page 2

Cybersecurity threats are an ongoing challenge for both the federal government and the private sector. For these reasons, I believe an investigation of the data security breach at Community Health Systems will help the Committee learn from these witnesses about security vulnerabilities they have experienced in order to better protect our federal information technology assets.

Thank you for your consideration of this request.

Sincerely,



Elijah E. Cummings
Ranking Member

switch/wp/2014/09/04/healthcare-gov-server-hacked-but-hhs-says-no-consumer-information-taken/) (reporting that although a test server was hacked, no personally identifiable information was compromised).

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MCHEENY, NORTH CAROLINA
W. JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALCHER, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUDITH ANAST, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT LUKATEL, TENNESSEE
TREV GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ISSA WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KATHY L. BENTLEY, MISSISSIPPI
RON DE SANTIS, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

Manitowish: (202) 225-5274
Faxes: (202) 225-5274
Minutemen: (202) 225-5274
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MEMBER

CAROLYN B. MALONEY, NEW YORK
CLEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WILL LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPECTER, CALIFORNIA
MATTHEW A. CARTY, PENNSYLVANIA
TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORNFORD, NEVADA
MICHELLE LUJAN GRISSMAN, NEW MEXICO
VACANCY

September 11, 2014

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am writing to request that the Committee hold a bipartisan hearing to examine a data security breach that may have compromised the personal information of millions of American consumers who shopped at Home Depot this year.

On Monday, Home Depot issued the following public statement:

The Home Depot, the world's largest home improvement retailer, today confirmed that its payment data systems have been breached, which could potentially impact customers using payment cards at its U.S. and Canadian stores.¹

Home Depot's statement highlighted "the increasing threat of cyber-attacks on the retail industry."² Press reports this week regarding this data security breach have warned that hackers "have for some time been scanning merchants' networks for ways to gain remote access, such as through outside contractors who have access to a computer network."³

Home Depot has more stores in the United States and a higher total annual sales volume than Target, which experienced a similar data security breach late last year. Home Depot operated 1,977 U.S. retail stores and had total sales of \$78.8 billion in fiscal year 2013.⁴ By

¹ Home Depot, *The Home Depot Provides Update on Breach Investigation* (Sept. 8, 2014) (online at <https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf>).

² *Id.*

³ *Home Depot Data Breach Could Be the Largest Yet*, New York Times (Sept. 8, 2014) (online at http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0).

⁴ Home Depot, *Form 10-K for the Fiscal Year Ended February 2, 2014* (online at <http://phx.corporate-ir.net/phoenix.zhtml?c=63646&p=irol-reportscurrent>) (filed Mar. 27, 2014).

The Honorable Darrell E. Issa
Page 2

comparison, Target operated 1,793 stores in the U.S. as of February 1, 2014, and had total sales of nearly \$73 billion in 2013.

Home Depot also appears to have experienced a data security breach for a longer period of time than the data security breach that occurred at Target. The data security breach at Target lasted from November 27 through December 15, 2013, and may have affected approximately 40 million credit and debit card accounts.⁵ According to press reports, the cyber-attack on Home Depot potentially "went unnoticed for as long as five months," and the total number of credit and debit card accounts that have been compromised is not yet known.⁶

Over the past year, the Committee has been investigating the security of the Healthcare.gov website. This investigation has involved numerous public hearings, more than a million pages of documents from federal agencies and private contractors, and 18 transcribed interviews. To date, however, no personally identifiable information has been compromised as a result of malicious cyber-attacks, although outside actors have repeatedly tried.⁷

Cybersecurity threats are ongoing challenges for both the federal government and the private sector. For these reasons, I believe an investigation of the data security breach at Home Depot will help the Committee learn from these witnesses about security vulnerabilities they have experienced in order to better protect our federal information technology assets.

Thank you for your consideration of this request.

Sincerely,


Elijah E. Cummings
Ranking Member

⁵ Target, *Form 10-K for the Fiscal Year Ending February 1, 2014* (online at <https://corporate.target.com/annual-reports/2013/10-K/form-10-K>) (filed Mar. 14, 2014).

⁶ *Home Depot Data Breach Could Be the Largest Yet*, New York Times (Sept. 8, 2014) (online at http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0).

⁷ See, e.g., *HealthCare.gov Server Hacked. But HHS Says No Consumer Information Taken*, Washington Post (Sept. 4, 2014) (online at www.washingtonpost.com/blogs/the-switch/wp/2014/09/04/healthcare-gov-server-hacked-but-hhs-says-no-consumer-information-taken/) (reporting that although a test server was hacked, no personally identifiable information was compromised).

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. CUCINIA, JR., TENNESSEE
PATRICK T. MCHENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TAM WALBERG, MICHIGAN
JANIS LANKFORD, OKLAHOMA
JUSTIN AMode, MICHIGAN
PAUL A. COUSE, ARIZONA
PATRICK MALLARD, PENNSYLVANIA
SCOTT DOWD, ARIZONA
TOMMY L. LEE, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DICK HASTINGS, WASHINGTON
PATRICIA M. LUMMIS, WYOMING
BOB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DAVID COLEMAN, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENNETT, MICHIGAN
NICK DANTES, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

Mo: 205-225-2674
Fax: 205-225-2874
E-mail: 205-225-2874
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MEMBER

CARDOLYN B. MALONEY, NEW YORK
CLEANER HOLMES, DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPOER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORNFORD, NEVADA
MICHELLE LILIAN GRISHAM, NEW MEXICO
VACANCY

September 15, 2014

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

On June 30, 2014, I wrote to request that the Committee conduct a transcribed interview of Sterling Phillips, the Chief Executive Officer of USIS. To date, you have not responded to my request. Based on troubling new revelations about USIS over the past several months, I now request that you issue a subpoena compelling Mr. Phillips to appear for a deposition. I am making this request for three reasons:

- (1) Mr. Phillips has been refusing for more than six months to respond to written questions from this Committee—sent under your signature—regarding alleged fraud committed by top USIS officials, and he has refused to provide the identities of executives at two USIS parent companies to allow the Committee to determine whether those officials knew about or directed fraudulent activities against U.S. taxpayers.
- (2) Cyber security experts have now briefed Committee staff on details of a malicious cyber attack against USIS this summer, raising serious new concerns about whether USIS has been complying with the requirements of its government contracts to secure the personally identifiable information of individuals applying for security clearances.
- (3) USIS apparently has been able to continue obtaining new federal contracts by exploiting a weakness in the current contracting award process.

The rest of this letter sets forth additional details about these issues and the need for Mr. Phillips to answer these questions at a deposition.

Refusal to Answer Committee Questions

Mr. Phillips testified at a hearing on February 11, 2014, regarding a \$1 billion civil suit brought in January by the Department of Justice alleging massive fraud by top USIS officials in

The Honorable Darrell E. Issa
Page 2

their background check contracts with federal agencies. In its filing, the Department stated that “USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company’s revenues and profits.”¹ The Department also stated that the previous CEO and other high-level USIS officials personally directed this “dumping” scheme:

USIS Senior Management was fully aware of and, in fact, directed the dumping practices. Beginning in at least March 2008, USIS’s President/CEO established the internal revenue goals for USIS. USIS’s Chief Financial Officer determined how many cases needed to be reviewed or dumped to meet those goals.²

As part of our investigation, we have been attempting to determine whether this alleged fraud scheme goes even higher. After USIS was acquired by Providence Equity Partners in 2007, the company adopted an aggressive new compensation plan to speed up its background investigations work. During the time period of the company’s alleged fraud from 2008 to 2012, Bill Mixon, who was the CEO at that time, received more than \$1 million in bonuses, and the company’s Chief Financial Officer received about \$470,000.

At the hearing in February, Mr. Phillips agreed that “bonuses awarded to the top officials at USIS during the alleged fraud were made according to a formula devised by the parent company, Altegrity.”³ In fact, USIS bonus policies were printed on Altegrity letterhead.⁴ In addition, Mr. Phillips stated that Altegrity’s Board of Directors “is comprised of principals with Providence Equity, the owners of the company.”⁵

However, Mr. Phillips did not provide the Committee with the identities of Altegrity’s Board of Directors or officials from Providence Equity Partners, stating instead: “I would have to look at the timing.”⁶

¹ United States’ Complaint, ¶ 42 (Jan. 22, 2014), United States of America ex rel. Blake Percival v. U.S. Investigations Services, Inc., M.D. Ala. (No. 11-CV-527-WKW).

² *Id.* at ¶ 51.

³ House Committee on Oversight and Government Reform, *Hearing on DC Navy Yard Shooting: Fixing the Security Clearance Process* (Feb. 11, 2014) (online at <http://oversight.house.gov/hearing/dc-navy-yard-shooting-fixing-security-clearance-process/>).

⁴ Minority Staff, House Committee on Oversight and Government Reform, *Contracting Out Security Clearance Investigations: The Role of USIS and Allegations of Systemic Fraud* (Feb. 11, 2014) (online at www.democrats.oversight.house.gov/uploads/USIS%20Security%20Clearance%20Report%2002-11-2014.pdf).

⁵ House Committee on Oversight and Government Reform, *Hearing on DC Navy Yard Shooting: Fixing the Security Clearance Process* (Feb. 11, 2014) (online at <http://oversight.house.gov/hearing/dc-navy-yard-shooting-fixing-security-clearance-process/>).

⁶ *Id.*

The Honorable Darrell E. Issa
Page 3

On March 18, 2014, you sent a follow-up letter to Mr. Phillips requesting that he provide answers to written questions I submitted after the hearing, including the identities of Alteryx's Board of Directors and Providence Equity Partners. You explained that the hearing record would remain open pursuant to "the direction of the Chairman."⁷

On April 10, 2014, in response to an inquiry from my staff, an attorney for Mr. Phillips sent an email stating: "The company does not anticipate making a further response."⁸ The refusal of Mr. Phillips to provide the identities of officials at two USIS parent companies prevents the Committee from fully investigating allegations of fraud against U.S. taxpayers.

Major Data Security Breach at USIS

On September 3, 2014, our staffs received a briefing from security experts at the Department of Homeland Security (DHS), the Office of Personnel Management (OPM), and the Office of the Director of National Intelligence who have been analyzing a major cyber attack that occurred against USIS computer systems this summer. Although much of the briefing was sensitive, there are several key points that may be discussed publicly.

First, although press accounts have reported that the attack may have compromised the personal information of up to 27,000 federal employees, government cyber security experts now believe this number is a floor—not a ceiling. The actual number of individuals affected by the USIS data security breach is not yet known, but these experts believe that the personal information of many more federal employees may have been compromised. USIS and other Alteryx subsidiaries received more than \$2 billion in federal contract work in recent years.⁹

Second, USIS data security measures appear to be inferior to those of the government. In March 2014, hackers also broke into the network of the Federal Investigative Service, a division of OPM that also conducts background investigations.¹⁰ Unlike USIS, the agency's data protection systems insulated personally identifiable information from the hackers, and cyber security experts believe no personally identifiable information was compromised.

⁷ Letter from Chairman Darrell E. Issa, House Committee on Oversight and Government Reform, to Sterling Phillips, Chief Executive Officer, USIS, LLC (Mar. 18, 2014) (online at <http://democrats.oversight.house.gov/uploads/QFR%27s%20Phillips-USIS%20-%20Security%20Clearances%202-11.pdf>).

⁸ Email from Attorney for Mr. Phillips, McDermott, Will & Emery, to Minority Staff, House Committee on Oversight and Government Reform (Apr. 10, 2014) (online at <http://democrats.oversight.house.gov/uploads/Redacted%202014-04-10%20Email%20from%20USIS%20Attys%20re%20QFR%20Response.pdf>).

⁹ Data based on search conducted on System for Award Management website (www.sam.gov/portal/SAM/#1) for Alteryx contracts with the federal government.

¹⁰ *Chinese Hackers Go After U.S. Workers' Personal Data*, Washington Post (July 10, 2014) (online at www.washingtonpost.com/world/national-security/chinese-hackers-go-after-us-workers-personal-data/2014/07/10/92db92e8-0846-11e4-8a6a-19355c7e870a_story.html).

The Honorable Darrell E. Issa
Page 4

New Contract Award to USIS

On July 17, 2014, I sent a bipartisan letter with Senator Tom Coburn to DHS requesting information about the process used to award a new contract to USIS, despite the fact that the Justice Department filed its fraud suit in January—six months earlier.¹¹

Federal acquisition regulations require agencies to review the past performance of potential contractors to ensure that they have a “satisfactory performance record” and a “satisfactory record of integrity and business ethics.”¹² On July 1, 2014, however, the U.S. Citizenship and Immigration Services within DHS awarded a new contract to USIS worth up to \$190 million to provide field office support services related to the operation of the Department’s immigration system.

According to DHS officials, USIS was able to obtain this contract because the company used a different “DUNS Number” for the subsidiary bidding for the DHS contract than it did for the subsidiary defending against the Justice Department fraud suit. As you know, DUNS is the Data Universal Numbering System maintained by Dun & Bradstreet to assign unique nine-digit identification numbers to businesses worldwide.¹³

As a result, it appears that USIS is able to continue obtaining federal contracts under the current procurement system if it has different DUNS numbers for different subsidiaries, despite the fact that the Justice Department has implicated the company’s entire upper management in a massive fraud scheme, and despite the fact that virtually nothing is known about the role of USIS parent companies in this scheme.

Request for Deposition

There are serious questions about the actions of top officials at USIS and its parent companies with respect to alleged fraud against U.S. taxpayers. A company that was supposed to be helping to secure our nation stands accused of dumping incomplete background check investigations to increase corporate profits, and now the personal information of tens of thousands of government workers seeking security clearances appears to have been compromised. Yet, USIS continues to obtain new contracts, and the CEO appears to believe he can ignore the Committee with impunity.

¹¹ Letter from Rep. Elijah E. Cummings, Ranking Member, House Committee on Oversight and Government Reform, and Senator Tom A. Coburn, M.D., Ranking Member, Senate Committee on Homeland Security and Governmental Affairs, to the Honorable Jeh Johnson, Secretary, Department of Homeland Security (July 17, 2014) (online at <http://democrats.oversight.house.gov/press-releases/cummings-and-coburn-send-bipartisan-inquiry-on-new-contract-to-usis-after-billion-dollar-fraud-suit/>).

¹² 48 C.F.R. § 9.104-1.

¹³ *About the DUNS Number*, Dun & Bradstreet (accessed Sept. 14, 2014) (online at <http://fedgov.dnb.com/webform/pages/dunsnumber.jsp>).

The Honorable Darrell E. Issa
Page 5

For all of these reasons, I respectfully request that you issue a subpoena to require Mr. Phillips to submit to a deposition with Committee staff. Thank you for your consideration of this request.

Sincerely,


Elijah E. Cummings
Ranking Member



OFFICE OF THE INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

December 15, 2014

The Honorable Blake Farenthold
Chairman, Subcommittee on Federal Workforce
U.S. Postal Service and the Census
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Farenthold:

We received your December 1 request for response to questions for the record by Mr. Gerald Connolly. Mr. Connolly's questions arose from testimony at the November 18, 2014 hearing titled, Examining Data Security at the United States Postal Service.

We have enclosed responses to Mr. Connolly's questions for the record.

Please let Wally Olihovik know if you need additional assistance on this or other matters. Mr. Olihovik can be reached at 703-248-2201.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tammy L. Whitcomb'. The signature is fluid and cursive, with the first name 'Tammy' being the most prominent.

Tammy L. Whitcomb
Deputy Inspector General

Enclosures

Questions for
Ms. Tammy Whitcomb
 United States Postal Service Office of Inspector General

Representative Gerald B. Connolly

November 19, 2014 Hearing
"Examining Data Security of the United States Postal Service"

1. Mr. Timothy Edgar's written testimony noted:

"The USPS can learn important lessons not only from past abuses involving mail monitoring, but from the actions of the government and industry in responding to recent surveillance controversies. Like the NSA, the USPS can adopt much more rigorous and detailed oversight of its handling of privacy requirements. Like Google and other technology companies, the USPS can publish periodic transparency reports detailing how many mail covers and warrants it processes each year, under what authorities, and how it addresses improper requests. The USPS should fight to make more, not less, information available about national security requests. The DNI is now providing yearly aggregate information about many such requests under national security authorities involving electronic surveillance; there is no reason such information should be withheld when it comes to monitoring the mail."

With respect to the suggested reforms above, if the United States Postal Service (USPS) refuses to adopt any or all of them, would you recommend that Congress consider enacting new statutory requirements to require USPS:

- Adopt much more rigorous and detailed oversight of its handling of privacy requirements;
- Publish periodic transparency reports detailing how many mail covers and warrants it processes each year, under what authorities, and how it addresses improper requests; and
- Provide reports detailing the annual or monthly aggregate information on how many national security requests USPS receives?

Response

Our audit work to date focused on the mail cover program policies and the adequacy of justifications, but not on the public reporting of information concerning mail covers and national security requests. We have completed one of two audits concerning the Postal Service mail cover program and will address the specific issues you raise in our second audit. Before we can make a recommendation with respect to public reporting we would need to allow the Postal Service and requesting agencies to voice any concerns they may have.

With regard to your concerns about USPS handling of privacy requirements, the Postal Service substantially revised its privacy policy in July 2014 but we have not yet done a critical review of the revised policy. However, we have noted in many of our prior work products that trust in the Postal Service is a critical asset which it must build and protect in all its work. We will consider delving more thoroughly into Postal Service privacy policies in the future, and at that point, we may have better information for you on the need for additional legislation.

Additionally, the Freedom of Information Act (FOIA) is a valuable transparency tool currently available to the public. Under FOIA, interested parties may request records regarding the number of mail covers and warrants to open mail processed by the Postal Service. It was a FOIA request that initiated much of the latest public discussion concerning Postal Service use of mail covers and mail imaging.

2. Please describe any additional statutory amendments you would recommend Congress consider related to enhancing USPS privacy protections, civil liberties safeguards, and transparency.

Response

The Office of Inspector General has not done any specific work that would indicate any amendments to existing Postal Service-specific privacy statutes are necessary. We would note, however, that the Privacy Act's definition of a "system of records", from 1974, has not been revised since the advent of computers and data analysis. As currently written, a "system of records" is "...a group of any records... from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual...." With search engines and full data retrieval capability, virtually any data retained in a database may be retrieved by name or identifying number. As we have suggested with respect to changes to the Computer Matching and Privacy Protection Act of 1988, it may be time to reconsider this aspect of the Privacy Act to ensure that it remains relevant in the digital age. We would also welcome a legislative effort to consolidate government-wide privacy protections in the Privacy Act.

Regarding work we have done to promote transparency, we made a recommendation for Postal Service management, "U. S. Purchasing Policies", (CA-AR-10-005, September 20, 2010), to fully and accurately track and publicly report competitive and noncompetitive contracting actions. The Postal Service began publishing an annual report in 2012 that contained information about both competitive and noncompetitive contract purchases valued at \$1 million and above. This report is available on the Postal Service's website.

3. At the hearing, the Postal Inspection Service emphasized that utilizing optical character recognition (OCR) applications to scan mail for routing purposes was a program completely separate from the Mail Covers Program. Please identify any statutory restrictions that would prohibit USPS, in the future, from utilizing any type of automated mail processing tool, such as mail imaging or Mail Isolation, Control, and Tracking (MICT) procedures, to support surveillance activities, or in any other way assist the Postal Inspection Service in carrying out its law enforcement related missions.

If no such statutory restrictions exist, would you recommend that Congress enact such statutory prohibitions to preclude potential future abuse?

Response

There are no statutes that prohibit the use of OCR technology to support surveillance activities. When mail is presented for imaging it is still, at that point, unsorted collection mail, and tracking specific mail to or from specific individuals, which is the essence of surveillance, would be extremely cumbersome at best. Processing images reveal almost nothing about a network of associates or mailing patterns or practices. However, in those very rare circumstances where there is a threat to public safety posed by the mail, mail imaging could provide valuable information to identify either potential victims or perpetrators.

In December, 2013, we issued "Management Alert – Mail Isolation, Control, and Tracking" (HR-MA-14-002) covering our work on the MICT program. We found that, currently, permission to use scanned mail images for investigative purposes is evaluated and granted by the VP Engineering, an unlikely position to address privacy questions. We found only infrequent use of the MICT capability, for what appear to be legitimate purposes. We did however, encourage the Postal Service to establish procedures for the coordination of mail tracking processes in the event of a suspicious mail incident including specific procedures and controls for using mail image information. We recommend that the new procedures be reviewed before a determination is made whether new legislation is required.

4. Has USPS shared with the Office of inspector General the Privacy Impact Assessment (PIA) that it conducted on the computer system used to process mail covers? If USPS has not conducted any Privacy Impact Assessments (PIAs), or hired an outside entity to conduct such PIAs on its behalf, of information technology that is directly or indirectly related to the Mail Covers Program; MICT; and mail imaging; would you recommend that Congress amend the law to require that USPS conduct such PIAs and publish them in an appropriate manner?

Response

The Postal Service did provide its Business Impact Assessment (BIA), which is equivalent to a PIA, for the mail cover program. Our review of the MICT program did not include an examination of the BIAs for MICT. USPS lists its BIAs on USPS.com. The website explains how the public may obtain a copy of the listed BIAs.

5. Congress authorized the U.S. Department of Homeland Security's U.S. Customs and Border Protection (CBP) to stop and search at the border, without a search warrant, mail of domestic origin transmitted for export by the United States Postal Service and foreign mail transiting the United States that is being imported or exported by the United States Postal Service. In addition, Federal Regulations establish that 100 miles in from an external boundary of the United States is a reasonable distance to establish a border zone in which CBP has the authority to conduct certain operations.

Thus, it is not clear that when the Postal Inspection Service receives a request from Federal law enforcement authorities, including CPB, to stop and search mail without a search warrant, and that is of domestic origin and transmitted for export by USPS, and that is physically located within 100 miles or less of an external boundary of the United States – whether USPS recognizes such a request as complying with Section 1583 of Title 19 of the United States Code, and accordingly, complies with such a request from a law enforcement agency, such as CBP, to conduct a warrantless search of such mail.

In the Office of Inspector General's view, under current law, is a request from CBP to conduct a warrantless search of mail that is delivered to a post office located in Hawaii, by a resident of Hawaii, and that is of domestic origin and transmitted for export by USPS, permitted and legal under Section 1583 of Title 19 of the United States Code, or any other statutory authority?

Response

Yes, it appears that the law permits CBP to search foreign destinating mail, over 16 ounces, in Hawaii, if the particular piece meets the requirements of Section 1583, and is within 100 miles of a U.S. border. 19 U.S.C. 1583 (as amended in 2002), provides for the warrantless search of mail sealed against inspection if:

- ***the sealed mail weighs over 16 ounces; and,***
- ***only where CBP determines there is reasonable cause to believe that the mail matter contains prohibited items listed in 19 U.S.C. 1583 (c)(1).***
- ***Under no circumstances may the communications contained within sealed mail be read without a warrant.***

- ***Pursuant to regulation, such searches may occur within 100 miles of an international border.***

"Mail Sealed Against Inspection" is defined by the Postal Service to include all domestic First Class Mail, including Express and Priority Mail, and most of the same categories of international mail.

6. It is not clear whether USPS collects and maintains statistics on how many times the Attorney General of the United States conducts physical searches of mail without prior judicial authorization, pursuant to the authority provided by Section 304(e) of the Foreign Intelligence Surveillance Act of 1978. Further, it is not clear whether USPS provides Congress with summary statistics on how many times the Attorney General has utilized this authority for all fiscal years in which the data exists; or alternatively, USPS is not aware of, and does not track, how often the Attorney General conducts physical searches of mail without prior judicial authorization, in accordance with FISA requirements.

If USPS does not do any of the tasks outlined above, would the Office of Inspector General consider recommending that Congress require USPS to collect, maintain, and disseminate in an appropriate manner, information on how often the Attorney General of the United States conducts physical searches of mail without prior judicial authorization, pursuant to the authority provided by Section 304(e) of the Foreign Intelligence Surveillance Act of 1978?

Response

The Office of Inspector General has not done any work in this area. However, this may be a report that would more properly be made by the Office of the Attorney General.

7. Please describe any policies and procedures that the Office of Inspector General is aware of USPS utilizing to ensure that the Mail Covers Program, or any other facet of the Postal Service, is not used, with or without authorization, to support a mail monitoring program, similar to HTLINGUAL. Do you believe that USPS utilizes rigorous and transparent processes, procedures, and controls to such an extent that the American public may be confident that there will not be a similar abuse of the Mail Covers Program as occurred several decades ago when USPS tacitly or explicitly cooperated with law enforcement and intelligence agencies to conduct illegal domestic surveillance?

Response

We note that the Mail Cover Regulations have been changed a number of times since the HTLINGUAL incidents, beginning in the 1950's to the 1970's,

which you reference. We recommended in our "Postal Inspection Service Mail Covers Program" (HR-AR-14-001, May 28, 2014) report that management improve controls to ensure responsible personnel process mail covers in a timely manner and conduct periodic reviews of the mail covers program. We also recommended management implement system controls to ensure data integrity in the Postal Inspection Service mail cover data system.

Further, we are currently conducting an audit of the Postal Service's Internal Mail Covers Program. Our objective is to determine whether the Postal Service and Postal Inspection Service are effectively and efficiently handling internal mail covers according to Postal Service and federal requirements. We will expand our audit to include an analysis of the changes to the regulations. At the conclusion of this audit we would be happy to meet with your staff to determine the need for additional legislation.

8. USPS remains a key component of American commerce, connecting our Nation even in our current digital age. As this hearing demonstrated, the activities of USPS, particularly the Postal Inspection Service, touch upon a wide range of industries, activities, and carry serious Constitutional implications.

However, Congress is hampered in its ability to conduct oversight of USPS because it does not recognize requests from an Office of a Member of Congress or certain Congressional Committees and Subcommittees as constituting official "requests by Congress." Thus, if a Member, such as the Chairman of the House or Senate Small Business Committee, inquires about Postal operations related to USPS customer privacy protections - a germane topic since a significant portion of regular USPS customers are American small businesses - USPS will not comply with such a request in an expeditious manner, and would likely direct the respective Chairs of the Small Business Committees to submit Freedom of Information Act requests, as any other individual would.

Do you believe that current USPS practice of adopting a highly constricted and limiting definition of what constitutes a request from Congress adversely impacts congressional oversight, hindering the ability of the individuals duly elected by our Nation's citizens to represent them, to effectively represent constituent's interests related to privacy rights and civil liberties?

Response

In FY 2011, we evaluated the Postal Service's Government Relations operations ("Government Relations Operations," FF-AR-11-014, September 23, 2011) to determine whether they were conducted efficiently and cost effectively. Government Relations is the Postal Service's primary liaison to government leaders and policy makers.

At that time, Government Relations did not have a comprehensive workload tracking and analysis system; therefore, we were unable to determine whether operations were performed effectively and efficiently and whether staffing levels appropriately matched the workload. Also, Government Relations did not maintain written policies and procedures for its operations.

We were unaware of the policy you cite, so would welcome the opportunity to learn more about these issues. We would also be happy to provide background on our prior audit work in this area.

HOUSE SUBCOMMITTEE ON FEDERAL WORKFORCE,
U.S. POSTAL SERVICE AND THE CENSUS

"Examining Data Security at the United States Postal Service"

November 19, 2014

*Post-Hearing Questions for the Record
Submitted to Chief Postal Inspector Guy J. Cottrell*

From Representative Gerald Connolly (D-VA):

1. Please describe in greater detail than offered in Section 233.3 of Title 39 of the Code of Federal Regulations the specific processes and procedures employed by the United States Postal Inspection Service in carrying out the Mail Covers Program.

Your response should address precisely what your statement meant in regard to the Mail Covers Program, "It's all done manually. The only electronic piece would be to actually photocopy the pieces of mail, that's the only electronic part of the process."

For example, does "manually" mean personnel copy data appearing on the outside cover of sealed or unsealed class of mail matter by hand, or do employees utilize computers to manually enter the data into an electronic database or another format?

Please confirm whether the Postal Inspection Service meant that it always executes mail covers manually (such as, but not limited to, photocopying or hand-copying), and please include in your response how USPS defines "manually" with respect to the Mail Covers Program.

Further, your answer should include a review of every piece of equipment that is utilized in carrying out the mail cover process.

Finally, if no automated processing equipment or asset is utilized in the manual process to obtain data under a mail cover, please identify any and all statutory or administrative requirements that would prevent the Postal Inspection Service from incorporating automated processing equipment into the Mail Covers Program in the future.

Answer:

As stated in my testimony and noted in 39 CFR § 233.3, a mail cover is the process by which a nonconsensual recording is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter (e.g., the name and address of the sender and addressee) or by which a record is made of the contents of any unsealed class of mail matter, for one of the following reasons:

- (i) To protect national security,
- (ii) To locate a fugitive,
- (iii) To obtain evidence regarding the commission or attempted commission of a crime, punishable by law by imprisonment for a term exceeding one year,
- (iv) To obtain evidence of a criminal violation or attempted criminal violation of a postal statute, or
- (v) To assist in the identification of property, proceeds or assets which are forfeitable because of a violation of criminal law.

Mail covers may be used as an investigative tool by other law enforcement agencies; however, a written request must be made through the U.S. Postal Inspection Service. Requesting law enforcement agencies must treat mail covers as restricted and confidential information. As with internal mail cover requests, outside law enforcement agencies must demonstrate reasonable grounds for requesting and using a mail cover. The requesting law enforcement agency must explain what criminal law the subject of the mail cover is violating and how the mail cover could further the investigation or provide evidence of a crime. Mail covers are authorized only when all requirements are met within the written request. The Postal Inspection Service reviews each request to ensure it contains enough information to stand alone, as full justification for the cover, and fully complies with all regulatory requirements. The Postal Inspection Service does not approve all submitted mail cover requests, and has denied both internal and external law enforcement mail cover requests for failing to meet program criteria.

Once a request for a regular mail cover is approved, the following steps occur to obtain the information:

- A letter to the Postmaster/Station Manager/Supervisor (depending on office size) is sent by personnel at the Criminal Investigations Service Center (CISC) in Chicago.
- The letter provides instructions on how to handle the recording of information including the name/address which is the subject of the mail cover.
- A Postal employee, generally the letter carrier assigned to the route, will then obtain the mail for the subject name/address.
- The Postmaster/Supervisor (or other assigned employee) will either, manually record the information on the appropriate form, or photocopy the mail and attach the copies to the form provided by the CISC.
- If the request was made by a Postal Inspector, the recorded mail cover information is sent to the Inspector directly. If the request was made by an outside law enforcement agency, the information is routed back through the CISC.

Mail covers may also be requested by Postal Inspectors for individual pieces of mail and investigative operations.

In limited circumstances, during an active investigation, if a physical mailpiece is no longer available, the Postal Inspection Service can request to obtain an image of the outside of a mailpiece from mail processing equipment. If the image of the mailpiece is available and deemed to play a vital role in the investigation, a mail cover is requested.

The term "manually" includes transcribing, photocopying, or photographing the information from the outside of mail matter or an image of mail matter. For single piece mail covers related to narcotics and dangerous mail investigations, mail piece information is manually entered into an Inspection Service database and a mail cover request is electronically generated.

We are not aware of any such statutory restriction that prevents the Inspection Service from incorporating automated processing equipment into the Mail Covers program, nor is the Inspection Service interested in doing so.

2. Please describe in greater detail how the United States Postal Service (USPS) counts mail covers that are reviewed and processed under the United States Postal Inspection Service's Mail Covers Program.

For example, when USPS receives a single request to conduct surveillance of five separate persons suspected of engaging in illegal activity, is that single request identifying five targets counted by USPS as five mail covers reviewed or a single mail cover reviewed?

Answer:

A mail cover request for a particular address will be counted as one mail cover regardless of the number of persons receiving mail. In the example posed above, if the five individuals resided at five different addresses, there would be five mail covers requested. If they reside at the same address, there would be one mail cover requested. Additionally, a procedure in connection with criminal investigations into dangerous mail and narcotics investigations was changed in late FY 2012. Prior to this change, a mail cover that was assigned to an investigative operation, regardless of the number of mailpieces, counted as a single mail cover. Under this new procedure, each mailpiece that is deemed to be part of an investigation receives a separate mail cover.

3. At the hearing, the Postal Inspection Service emphasized that utilizing optical character recognition (OCR) applications to scan mail for routing purposes was a program completely separate from the Mail Covers Program.

Please identify any specific statutory requirements that prohibit USPS from utilizing a mail processing tool, such as mail imaging, in[a] manner to conduct surveillance or in any other way assist the Postal Inspection Service in carrying out its mission.

Further, please identify any specific statutory requirements that prohibit USPS from utilizing the Mail Isolation, Control and Tracking (MICT) safety procedures to assist the Postal Inspection Service in carrying out the Mail Covers Program.

If no statutory prohibitions exist preventing the expansion in the manner and use of mail imaging and MICT tools, please explain why the USPS does not utilize these assets. Does the Postal Inspection Service lack the technical means to do so? Are there other reasons and justifications precluding the Postal Inspection Service from engaging in this type of data mining to assist its law enforcement activities, including, but not limited to, the Mail Covers Program.

Answer:

The Privacy Act and the mail cover regulations place limitations on the type of information the Postal Service can obtain, how that information can be used, how long it may be maintained and under what circumstances, if any, such information can be disseminated.

In limited circumstances, during an active investigation, if a physical mailpiece is no longer available, the Postal Inspection Service can request to obtain an image of the outside of the mailpiece from mail processing equipment. If the mailpiece is deemed to play a vital role in the investigation, a mail cover is requested.

Mail Isolation, Control and Tracking (MICT) is a set of safety procedures developed in response to the anthrax mailings that occurred in October of 2001. The purpose of these procedures is to protect Postal Service employees and the American public in the event a known contaminated piece of mail has been processed through postal equipment. MICT is only triggered when a potentially contaminated mailpiece is identified, and the ultimate goal is to be able to trace the path of the contaminated mailpiece through the mail processing system so that the facilities, vehicles and processing machines that came in contact with the mailpiece can be isolated and appropriate safety measures can be taken. Generally, the tracking is accomplished by barcode information that is placed on the mailpiece during processing. Once the path of a contaminated mail piece has been determined, appropriate safety measures can be taken. Safety is the ultimate goal of MICT, not "surveillance".

MICT is not used in connection with the mail cover program; and, neither the mail cover program nor MICT are a form of data mining.

If the Postal Inspection Service does not always execute mail covers manually, please:

- a) Identify all instances where the Postal Inspection Service utilized, or utilizes automated tools, such as OCR-enabled scanners, in support of the Mail Covers Program; and

Answer:

As previously stated, in limited circumstances, during an active investigation, if a physical mailpiece is no longer available, the Postal Inspection Service can request to obtain an image of the outside of a mailpiece from mail processing equipment. If the mailpiece is deemed to play a vital role in the investigation, a mail cover is requested.

The Postal Inspection Service does not use automated tools, to support the Mail Cover program.

- b) Provide statistics that address what percentage of mail covers involved solely, or primarily, manual execution, and what percentage of mail covers were solely, or primarily, executed through electronic means; for all fiscal years in which the data exists.

Answer:

As previously mentioned, mail covers are not executed electronically; therefore we do not have data that is responsive to this question.

4. Please explain why the Postal Inspection Service does not currently make publicly available summary statistics on the Mail Covers Program that provide the annual number of total mail covers USPS receives and approves, in addition to identifying the originating agency making the request.

If applicable, please identify the specific statutory provision that prohibits USPS from providing these summary statistics.

Further, if there is no statutory prohibition, please explain whether USPS is willing to immediately begin providing these summary statistics in a format that is accessible and regular updated for accuracy. Why or why not?

Answer:

Although we are not aware of any statutory prohibitions, because of the sensitivity of law enforcement information and consistent with state and federal law enforcement practices, we do not make publicly available statistical information regarding law enforcement investigative techniques, or provide particulars about law enforcement sensitive information collected during an investigation. Also, generally, we do not publicly identify law enforcement agencies who have requested such information. We would be willing to publish general statistical information regarding the mail cover program, if required.

5. Please provide, in their entirety, any Privacy Impact Assessments (PIA) that USPS has conducted, or hired an outside entity to conduct on its behalf, of information technology that is directly or indirectly related to the Mail Covers Program; MICT; and mail imaging.

If no such PIAs exist, please explain why USPS does not believe such PIAs are necessary, and what alternative methods USPS employs to ensure the American public has transparency into the utilization of these tools and the Mail Covers Program.

Answer:

Due to the sensitive nature of responsive materials associated with this request, we will provide this information to the Subcommittee under separate cover.

6. Congress authorized the U.S. Department of Homeland Security's U.S. Customs and Border Protection (CBP) to stop and search at the border, without a search warrant, mail of domestic origin transmitted for export by the United States Postal Service and foreign mail transiting the United States that is being imported or exported by the United States Postal Service.

In addition, Federal Regulations establish that 100 miles in from an external boundary of the United States is a reasonable distance to establish a border zone in which CBP has the authority to conduct certain operations.

When the Postal Inspection Service receives a request from Federal law enforcement authorities, including CBP, to stop and search mail without a search warrant, and which is of domestic origin and transmitted for export by USPS, and which is physically located within 100 miles or less of an external boundary of the United States — does USPS recognize this request as complying with Section 1583 of Title 19 of the United States Code, and does USPS comply with such a request from CBP to conduct a warrantless search of such mail?

For example, if a resident of Hawaii delivers mail to a post office located in Hawaii that is of domestic origin and transmitted for export by USPS, would USPS recognize—even in theory—that a request from CBP to conduct a warrantless search of such mail is permitted and legal under Section 1583 of Title 19 of the United States Code, or any other statutory authority?

Does USPS collect and maintain statistics on how many times the Attorney General of the United States conducts physical searches of mail without prior judicial authorization, pursuant to the authority provided by Section 304(e) of the Foreign Intelligence Surveillance Act of 1978?

In addition, if the answer is yes to the question above, please provide summary statistics on how many times the Attorney General has utilized this authority for all fiscal years in which the data exists.

Alternatively, if the answer is no, please provide a detailed justification for why USPS is not aware of, and does not track, how often the Attorney General conducts physical searches of mail without prior judicial authorization, in accordance with FISA requirements.

Answer:

Although courts have recognized extended border searches by Customs and Border Protection as it relates to searches of mail away from physical borders or functional equivalents of borders, for purposes of complying with 19 U.S.C. § 1583, the USPS presents domestic origin, foreign destination mail to U.S. Customs for their inspection and/or warrantless search at one of five designated sites. These Postal Service facilities are located at the following airports: John F. Kennedy International Airport, New York (JFK), Los Angeles International Airport (LAX), O'Hare Airport, Chicago, IL (ORD), San Francisco International Airport (SFO) and Miami International Airport (MIA).

The Inspection Service does track searches of mail pursuant to Section 304(e) of the Foreign Intelligence Act of 1978. Any information related to these searches should be directed to the United States Attorney General's Office.

7. Please describe precisely what policies and procedures USPS utilizes to ensure that the Mail Covers Program, or any other facet of the Postal Service, is not used, with or without authorization, to support a mail monitoring program, similar to HTLINGUAL. Why should the American public have confidence that there will not be similar abuse of the Mail Covers Program as occurred several decades ago?

Answer:

The Postal Service does not have a mail monitoring program and has no interest in establishing one. The Postal Service has regulations and policies in place to protect against such abuse. In addition to the Mail Cover regulations at 39 CFR § 233.3, the policies from the Postal Service's Administrative Support Manual set strict rules to protect the sanctity of sealed and unsealed mail, and personal information appearing on the outside of mailpieces. These policies state that opening, searching, and reading of mail is generally prohibited. Sealed and unsealed mail is protected against inspection, with only limited exceptions, including: consent of the addressee or sender, a search warrant, or mail reasonably suspected of being dangerous to persons or property. Unsealed mail may also be opened by a postal employee authorized to make a determination about mail ability or postage.

Additionally, as a general rule of Postal policy, Postal Service employees may not disclose information or data from the exterior of a piece of mail, disclose information about the contents of a piece of mail, or disclose other information about a piece of mail, to other individuals within or outside the Postal Service. Only limited exceptions allow for disclosure of such information, including: when the Postal Inspection Service or Office of the Inspector General have a reasonable basis to suspect that the information is evidence of the commission of a crime; in accordance with the mail cover regulations; as mandated by a search warrant; as mandated by a federal court order; to fulfill the request of the sender or addressee; for specified postal operations; or to ensure the health or safety of Postal Service employees or the public.

In addition to training regarding these regulations, discipline up to and including removal can be imposed on employees who violate laws or regulations. Furthermore, the Privacy Act includes possible criminal penalties for individuals who violate the privacy protections afforded under the Act.

8. The Postal Inspection Service attributed the 2013 spike in the number of mail covers to a narcotics investigation. Approximately 40,000 mail covers that year were attributed to this particular investigation. Does this mean 40,000 individuals were subject to a mail cover?

Answer:

As stated during my testimony, the trend over the past five years indicate a continued reduction in the use of mail covers by outside law enforcement agencies. This trend is consistent with the decreased use of mail covers by the Postal Inspection Service, with one significant exception. In late FY 2012, the Postal Inspection Service revised mail cover procedures in connection with criminal investigations into dangerous mail and narcotics investigations. This procedural change, whereby we assigned mail covers to individual pieces of mail as opposed to an operation, drove the increase in the total number of mail covers. Prior to this procedural change, one mail cover would blanket an operation which may have consisted of multiple mailpieces. This change allows us to better track the number of mailpieces in criminal investigations, as noted in the table below:

Mail Covers by Category	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014
Inspector Mail Covers	3391	3195	3187	2848	2824
Outside Agency Mail Covers	9462	9233	8265	6732	6274
One-Day Mail Covers	4956	4327	4652	41102	48095
Total Mail Covers	17809	16755	16104	50682	57193
Mail Volume (Billions)	170.9	168.3	159.9	158.4	155.4

9. The Postal Inspection Service produces internal reports on the Mail Covers Program.

a) Please identify all personnel and positions that are authorized to view these internal reports;

Answer:

The Postal Inspection Service does not routinely produce reports on mail covers; rather, based on need or upon request, the Inspection Service can produce limited internal statistical reports to aid in productivity. Postal Inspection Service and Office of Inspector General employees with appropriate security clearances, including Postal Inspectors, Mail Cover Unit personnel, Office of Counsel personnel, Criminal Investigations Service Center manager and program specialists, some Information Technology personnel, and OIG auditors have access to the system which is capable of generating reports.

- b) Please explain how these reports are shared with Congress, including the frequency with which they are transmitted to the Legislative Branch; and

Answer:

The Postal Inspection Service does not routinely produce reports on mail covers; rather, based on need or upon request, the Inspection Service can produce limited internal statistical reports to aid in productivity. Therefore reports of this nature are not shared with Congress.

- c) Please justify why USPS does not release the internal reports to the public.

Answer:

The Postal Inspection Service does not routinely produce reports on mail covers and the release of this information could compromise law enforcement activities as well as the safety of law enforcement personnel and Postal employees.

10. Please provide data on how often mail-covered mail is opened without a warrant for any fiscal years in which the data exists.

Answer:

A mail cover does not allow for a mailpiece to be opened. All mail, including mail subject to a mail cover, and that which is sealed against inspection, cannot be opened by the Inspection Service without the issuance of a Federal Search Warrant, or under other limited circumstances, including consent from the sender or addressee and mail reasonably suspected of being dangerous to persons or property.

The Postal Service does not routinely produce reports on how often mail-covered mail is opened without a warrant. Although these limited occurrences are recorded in the narrative of the investigative report, there is no searchable field that allows the Inspection Service to readily retrieve this data. Information of this sort would require a manual review of each possible occurrence within any given fiscal year.

11. Please provide what percentage of mail covers are letters and what percentage are parcels.

Answer:

We do not keep statistics for this type of information.

12. Did the Postal Inspection Service identify specific entities that were responsible for 20 percent of mail covers being approved improperly because of a lack of written authorization, and 13 percent being approved without sufficient justification?

Please describe how the Postal Inspection Service held the responsible entities accountable for the troubling compliance incident rate reported by the Office of Inspector General.

Answer:

The Inspection Service's Criminal Investigations Service Center (CISC) is the operation responsible for administering the non-national security mail covers. The improper approvals identified during the OIG audit were attributable to a lack of written delegation of authority from the CISC Manager. This has been corrected and the written delegations have been issued. The "lack of sufficient justification" issue has also been addressed, and it was determined sufficient justification had been provided in the instances noted, but was not completely transcribed into the mail cover file. Corrective measures have been implemented to prevent a recurrence. Additionally, updated training materials and procedures are being prepared for those involved in the administration of the program.

13. Please provide an answer in the affirmative or the negative ("yes" or "no"), along with a detailed explanation to the following question:

When USPS receives a request from a Member of Congress, does USPS consider this request to be a "request from Congress"?

If the USPS does not believe that a request from a Member of Congress constitutes a "request from Congress" please explain why, and clearly delineate all instances in which USPS would recognize a request as constituting a "request from Congress." In addition, please specifically provide a yes or no answer to the following questions related to USPS views on this topic:

Does USPS consider a request from the Chairman of the House Small Business Committee to be a "request from Congress"?

Does USPS consider a request from the Chairman of the Energy and Commerce Committee to be a "request from Congress"?

Does USPS consider a request from the Chairman of the Senate Small Business Committee to be a "request from Congress"?

Does USPS consider a request from the Chairman of the Senate Commerce Committee to be a "request from Congress"?

Does USPS consider a request from the Chairmen of the House or Senate Appropriations Committees to be a "request from Congress"?

Answer:

We interpret this question as asking when a request is considered a request from "Congress" for purposes of the Freedom of Information Act (FOIA) (5 U.S.C. § 552(d)) and the Sunshine Act (5 U.S.C. § 552b(l)).

No, a request from an individual Member of Congress is not treated as a request from "Congress" under FOIA or the Sunshine Act. Individual Members are treated like any other requester under these statutes. This practice accords with the Executive Branch's long-standing interpretation of FOIA. See *Department of Justice Guide to the Freedom of Information Act, Procedural Requirements* at 18 (2013) (noting that "individual members of Congress possess the same rights of access as those guaranteed to 'any person.'" (citing FOIA Update, "Congressional Access under FOIA," Vol. V, No. 1, at 3-4 (1984)). As DOJ has noted, there is a fundamental distinction between "Congress" as an institution, acting through either House of Congress or through delegations of authority to committees, and individual Members of Congress. This distinction is also recognized in the *Congressional Oversight*

Manual published by the Congressional Research Service (CRS). See Frederick M. Kaiser, Walter J. Oleszek, Todd B. Tatelman, *Congressional Oversight Manual*, CRS Report No. RL30240, at 55-57 (2011).

Therefore, a request under FOIA is treated as a request from "Congress" if the request is made by either House of Congress, or on behalf of a committee or subcommittee acting within the scope of its delegated jurisdiction. The same approach applies to the parallel provision of the Sunshine Act.

A request by the Chairman of the listed committees could potentially qualify as a request from "Congress" for purposes of FOIA and the Sunshine Act. However, a precise answer would depend on the specific information requested, and whether the subject matter falls within the delegated jurisdiction of the committee. See, e.g., *Congressional Oversight Manual* at 24 (noting that committees "have only the power to inquire into matters within the scope of the authority delegated to them by their parent body," and that "[e]stablishing committee jurisdiction is the foundation for any attempt to obtain information and documents from the Executive Branch.")

Timothy H. Edgar

Answers to Questions for the Record

November 19, 2014 Hearing:
 “Examining Data Security at the United States Postal Service”

Questions from Rep. Gerald E. Connolly.

1. Your written testimony noted:

“The USPS can learn important lessons not only from past abuses involving mail monitoring, but from the actions of the government and industry in responding to recent surveillance controversies. Like the NSA, the USPS can adopt much more rigorous and detailed oversight of its handling of privacy requirements. Like Google and other technology companies, the USPS can publish periodic transparency reports detailing how many mail covers and warrants it processes each year, under what authorities, and how it addresses improper requests. The USPS should fight to make more, not less, information available about national security requests. The DNI is now providing yearly aggregate information about many such requests under national security authorities involving electronic surveillance; there is no reason such information should be withheld when it comes to monitoring the mail.”

With respect to the suggested reforms above, if the United States Postal Service (USPS) refuses to adopt any or all of them, would you recommend that Congress enact new statutory requirements to require that USPS:

- Adopt much more rigorous and detailed oversight of its handling of privacy requirements;
- Publish periodic transparency reports detailing how many mail covers and warrants it processes each year, under what authorities, and how it addresses improper requests; and
- Provide reports detailing the annual or monthly aggregate information on how many national security requests USPS receives?

Response

The answer is yes, I would favor legislation if the U.S. Postal Service (USPS) does not voluntarily adopt significant reforms to protect privacy.

The U.S. Postal Service has not (yet) adequately protected its customers’ privacy or the public’s right to know. First, it has not adequately overseen its own privacy requirements or enforced its own rules when it comes to mail covers. Only detailed and rigorous internal oversight of the program will correct this. The Inspector General has provided excellent recommendations in this area. Congress should hold USPS to these recommendations and, if legislation is necessary, be prepared to act.

Second, USPS has (still) not provided sufficient transparency to the public in how it handles mail covers, particularly those involving national security. While such requests are obviously sensitive, the USPS should provide at least the same level of transparency

regarding national security requests as the intelligence community has provided regarding foreign intelligence surveillance. This would involve providing aggregate annual numbers regarding how many requests are made, and how many postal customers these requests affect. If USPS is not willing to provide at least this level of transparency on its own, Congress should consider legislation.

2. Please describe any additional statutory amendments you would recommend to Congress related to enhancing USPS privacy protections, civil liberties safeguards, and transparency.

Response

If USPS is unable to correct the deficiencies in its mail covers program with additional oversight and transparency, Congress may want to consider imposing some form of judicial check on this tool. Police must obtain a court order to install a pen register or trap and trace device – called a PR/TT order – to obtain communications metadata. Postal metadata does not require any judicial order. Instead, the public expects the USPS to insist that proper procedures are followed in order to protect its customers' privacy. If USPS is unable to do so, it may be prudent for Congress to require a court order for collection of what amounts to postal metadata.

3. At the hearing, the Postal Inspection Service emphasized that utilizing optical character recognition (OCR) applications to scan mail for routing purposes was a program completely separate from the Mail Covers Program.

In the event that there are statutory restrictions that would prohibit USPS from utilizing any type of automated mail processing tool, such as mail imaging or Mail Isolation, Control, and Tracking (MICT) procedures, to support surveillance activities, or in any other way assist the Postal Inspection Service in carrying out its law enforcement related missions, would you recommend that Congress enact such statutory prohibitions to preclude potential future abuse?

Response

There is some comfort in knowing that the USPS has not linked its mail covers program to the automated mail imaging technology it uses to support routing the mail – at least not yet. By keeping these two functions separate, USPS ameliorates to some extent the concerns that I expressed in my written statement about maintaining what amounts to a bulk database of all Americans' mail covers, similar to the NSA bulk database of Americans' phone records.

However, the security and privacy problems associated with the bulk imaging of the outside of items of mail for routing purposes are significant even without a direct link to the mail covers program. For example, the database is still potentially a target for hackers even if it is not available for law enforcement or intelligence requests.

In addition, access to the database for surveillance purposes is limited only by USPS's own internal decision not to coordinate its mail imaging software with its mail covers program. In some ways, bulk collection of postal metadata for routing purposes, without a link to the mail covers program, offers the worst of both worlds. There are

privacy and security concerns with the database, but legitimate mail covers must still be executed by hand.

Keeping the postal imaging data and mail covers programs separate will not, therefore, guarantee either privacy or security in the long run. Instead, it would be preferable to tighten security of the postal imaging data – by ensuring such data is retained for only as long as necessary, for example. Congress might also consider legislation ensuring that, if these programs were ever linked together, mail covers would still require individual suspicion, and forbidding any kind of data mining or pattern analysis of postal imaging data.

4. If USPS has not conducted any Privacy Impact Assessments (PIAs), or hired an outside entity to conduct such PIAs on its behalf, of information technology that is directly or indirectly related to the Mail Covers Program; MICT; and mail imaging; would you recommend that Congress amend the law to require that USPS conduct such PIAs?

Response

Privacy Impact Assessments (PIAs) can be a useful tool in analyzing programs and systems that pose privacy concerns. When I was in government, I was involved in drafting and reviewing PIAs for intelligence and homeland security programs. Many of these PIAs were not required by law, but were conducted by agencies on a voluntary basis. There is no reason USPS cannot do so as well.

Congress should encourage USPS to conduct PIAs for each of the programs you mentioned – mail covers, MICT, and mail imaging. If USPS does not conduct such PIAs on a voluntary basis, legislation may be required.

5. Congress authorized the U.S. Department of Homeland Security's U.S. Customs and Border Protection (CBP) to stop and search at the border, without a search warrant, mail of domestic origin transmitted for export by the United States Postal Service and foreign mail transiting the United States that is being imported or exported by the United States Postal Service. In addition, Federal Regulations establish that 100 miles from an external boundary of the United States is a reasonable distance to establish a border zone in which CBP has the authority to conduct certain operations.

Thus, it is not clear that when the Postal Inspection Service receives a request from Federal law enforcement authorities, including CBP, to stop and search mail without a search warrant, and which is of domestic origin and transmitted for export by USPS, and which is physically located within 100 miles or less of an external boundary of the United States – whether USPS recognize such a request as complying with Section 1583 of Title 19 of the United States Code, and accordingly, complies with such a request from a law enforcement agency, such as CBP, to conduct a warrantless search of such mail.

In your opinion, do you believe that under current law, a request from CBP to conduct a warrantless search of mail delivered to a post office located in Hawaii, by a resident of Hawaii, and that is of domestic origin and transmitted for export by USPS, would be permitted and legal under Section 1583 of Title 19 of the United States Code, or any other statutory authority?

Response

The short answer is no, not without a warrant – not if the item that CBP wants to examine is a letter, as opposed to a package. While it is correct that 19 U.S.C. § 1583 permits U.S. Customs and Border Protection to search some items of mail at the international border without a warrant, there are important limitations on this authority.

First, section 1583 does not permit warrantless searches of mail sealed against inspection that weigh sixteen ounces or less. For mail in excess of sixteen ounces, the authority to search for customs purposes is limited by a provision that prohibits reading any correspondence without a search warrant. These limitations ensure that the contents of a person's correspondence, even at the border, remains protected against warrantless search.

This rule is in keeping with the decision, made by the administration of George Washington, that the United States would keep sacrosanct the privacy of mail – including international mail – rather than establish secret rooms to open and read such mail for intelligence or security purposes.

6. It is not clear whether USPS collects and maintains statistics on how many times the Attorney General of the United States conducts physical searches of mail without prior judicial authorization, pursuant to the authority provided by Section 304(e) of the Foreign Intelligence Surveillance Act of 1978. Further, it is not clear whether USPS provides Congress with summary statistics on how many times the Attorney General has utilized this authority for all fiscal years in which the data exists; or alternatively, USPS is not aware of, and does not track, how often the Attorney General conducts physical searches of mail without prior judicial authorization, in accordance with FISA requirements.

If USPS does not do any of the tasks outlined above, would you recommend that Congress require USPS to collect, maintain, and disseminate in an appropriate manner, information on how often the Attorney General of the United States conducts physical searches of mail without prior judicial authorization, pursuant to the authority provided by Section 304(e) of the Foreign Intelligence Surveillance Act of 1978?

Response

It would be useful to keep track of the number of FISA-authorized physical searches of mail, at least for purposes of internal compliance and review and to facilitate Congressional oversight. It should be noted that in the event that FISA searches are conducted without prior judicial authorization, FISA does require subsequent approval. In either case, the number of such searches (emergency or with prior FISA court approval) should be tracked.

The Office of the Director of National Intelligence is now issuing an annual transparency report with information regarding the number of targets affected on an annual basis by national security authorities, including FISA physical searches. The intelligence community may have valid national security concerns about breaking down the number of FISA physical searches further into particular types of searches, such as searches of

mail. If searches of physical mail involve only a very small number of FISA investigations, there may be valid concerns that detailed public reporting might compromise such investigations.

At a minimum, however, USPS should have the ability – and should – report some information about how it is handling government requests under various authorities (law enforcement and national security), in the same way as large technology companies like Google and telecommunications providers now do.

7. Please describe any policies and procedures that you are aware of USPS utilizing to ensure that the Mail Covers Program, or any other facet of the Postal Service, is not used, with or without authorization, to support a mail monitoring program, similar to HTLINGUAL. Based on your current understanding of USPS operations, do you believe the American public may be confident that there will not be similar abuse of the Mail Covers Program as occurred several decades ago?

Response

The question that concerns me is not whether USPS has law and policy that protects Americans' privacy – it seems to me that it does – but the degree of laxity in adhering to existing policies that was reflected in the Inspector General report that was the subject of the hearing.

HTLINGUAL was illegal at the time and was understood to be illegal by everyone who fully understood the program. The main lesson I draw from the HTLINGUAL episode is that the USPS cannot afford to defer to law enforcement or national security officials in how it handles requests, because USPS has a unique responsibility to ensure privacy of the mail.

USPS made commitments at the hearing, and earlier, to respond to the findings of the Inspector General. If USPS honors those commitments, it will do a great deal to restore public trust.

8. USPS remains a key component of American commerce, connecting our Nation even in our current digital age. As this hearing demonstrated, the activities of USPS, particularly the Postal Inspection Service, touch upon a wide range of industries, activities, and carry serious Constitutional implications.

However, Congress is hampered in its ability to conduct oversight of USPS because it does not recognize requests from an Office of a Member of Congress or certain Congressional Committees and Subcommittees as constituting official "requests by Congress." Thus, if a Member, such as the Chairman of the House or Senate Small Business Committee, inquires about Postal operations related to USPS customer privacy protections – a germane topic since a significant portion of regular USPS customers are American small businesses – USPS will not comply with such a request in an expeditious manner, and would likely direct the respective Chairs of the Small Business Committees to submit Freedom of Information Act requests, as any other individual would.

Do you believe that current USPS practice of adopting a highly constricted and limiting definition of what constitutes a request from Congress adversely impacts congressional

oversight, hindering the ability of the individuals duly elected by our Nation's citizens to represent them, to effectively represent constituents' interests related to privacy rights and civil liberties?

Response

I would strongly urge the USPS to drop this tactic and to work with Members of Congress to get them what they need to perform their legitimate oversight functions. Congressional oversight is an essential element in restoring and maintaining public trust. While I was in government, I worked hard to ensure responsiveness to oversight requests involving some of our nation's most sensitive programs. Where we needed additional time, or had valid concerns of privilege or national security, we tried to work in good faith to get Members of Congress what they needed. It does not serve the public interest, or even the narrower interest of a government agency, to respond to Congressional oversight grudgingly or to play word games.